Journal für die reine und angewandte Mathematik

gegründet von A. L. Crelle 1826

Herausgegeben von

Helmut Hasse

Band 182

Heft 3/4

Vorträge
der Vortragswoche über Gruppentheorie
Göttingen, 26.—30. Juni 1939

Ausgegeben am 21. September 1940

Walter de Gruyter & Co.

vormals G. J. Göschen'sche Verlagshandlung / J. Guttentag, Verlagsbuchhandlung / Georg Reimer / Karl J. Trübner / Veit & Comp.

Berlin 1940

Band 182. Heft 3/4.

Inhaltsverzeichnis.

	Seite
Vortragswoche über Gruppentheorie, Göttingen 1939	129
Hall, P., The classification of prime-power groups	130
Magnus, Wilhelm, Über Gruppen und zugeordnete Liesche Ringe	142
Zassenhaus, Hans, Darstellungstheorie nilpotenter Lie-Ringe bei Charakteristik $p > 0$	150
Hall, P., Verbal and marginal subgroups	156
Grün, O., Zusammenhang zwischen Potenzbildung und Kommutatorbildung	158
Speiser, Andreas, Gruppen aus der Klassenkörpertheorie	178
Wielandt, Helmut, p-Sylowgruppen und p-Faktorgruppen	180
Hall, P., On groups of automorphisms	194
Witt, Ernst, Die Automorphismengruppen der Cayleyzahlen	205
Hall, P., The construction of soluble groups	206
van der Waerden, B. L., Bericht über die Arbeit von H. Fitting: Beiträge zur Theorie der Gruppen endlicher Ordnung	215
Scholz, Arnold, Zur Abelschen Durchkreuzung	216
——, Totale Normenreste, die keine Normen sind, als Erzeuger nichtabelscher Körpererweiterungen. II	217
Krull, Wolfgang, Über separable, abgeschlossene Abelsche Gruppen	235
Specht, Wilhelm, Darstellungstheorie der endlichen Gruppen	242

An unsere Mitarbeiter!

Es ist unbedingt notwendig, daß alle zur Einsendung gelangenden Manuskripte sowohl vollkommen druckfertig, als auch in gut lesbarer, möglichst Maschinen-Schrift gehalten sind, wobei die gotischen und griechischen wie überhaupt alle besonderen Typen durch Buntstift bezeichnet werden. Nachträgliche Korrekturen verursachen wesentliche Kosten, die sich naturgemäß auf die Preisgestaltung des Journals mit auswirken müssen. Machen sich also aus irgendeinem Grunde Textänderungen eines Beitrages notwendig, so sind diese der Schriftleitung sofort mitzuteilen, wenn sie die endgültige Annahme und Weitergabe an den Verlag meldet; Korrekturen nach dem Vorliegen des Satzes dürfen sich ausschließlich auf die Verbesserung von Satzfehlern erstrecken.

Manuskripte, die den eingangs erwähnten Vorschriften entsprechen, ermöglichen auch der Schriftleitung eine raschere Prüfung als schwer leserliche und können infolgedessen schneller zum Druck gelangen.

Im Interesse des schnellen Erscheinens der einzelnen Hefte erhalten die Herren Verfasser grundsätzlich nur eine Korrektur ihrer Beiträge. Da seitens der Schriftleitung die Korrekturen in typographischer Hinsicht sorgfältige Lesung finden und die richtige Ausführung der Autor-Korrekturen genau überwacht wird, hoffen wir, auch so allen Wünschen gerecht zu werden.

Die Herren Verfasser erhalten von allen Abhandlungen 75 Sonderabdrucke kostenfrei, weitere gegen Berechnung.

Sendungen für das Journal erbittet die Schriftleitung unter der Anschrift:
An die Schriftleitung des Journals für die reine und angewandte Mathematik
Professor Dr. Helmut Hasse, Göttingen, Mathematisches Institut, Bunsenstr. 3-5.

Druck von Walter de Gruyter & Co., Berlin W 35
Printed in Germany

Vortragswoche über Gruppentheorie, Göttingen 1939.

Im Mathematischen Institut Göttingen fand in der Zeit vom 26.—30. Juni 1939 eine

Vortragswoche über Gruppentheorie

statt.

Im Mittelpunkt dieser Veranstaltung stand eine Vortragsreihe von Philip Hall, Cambridge (England). Außerdem hielten Andreas Speiser, Zürich (Schweiz), sowie eine Reihe deutscher Mathematiker Einzelvorträge. Der Vortragsplan war:

Montag, 26. Juni

10—12 P. Hall, Cambridge, Classification of prime-power groups.
17—18 W. Magnus, Königsberg, Zuordnung von Lieschen Ringen zu Gruppen.
18—19 H. Zassenhaus, Hamburg, Nilpotente Liesche Ringe und p-Gruppen.

Dienstag, 27. Juni

10—11 P. Hall, Cambridge, Earlier work on prime-power groups.
11—12 O. Grün, Berlin, Über den Zusammenhang zwischen Potenzbildung und Kommutatorbildung.
17—18 A. Speiser, Zürich, Gruppen aus der Klassenkörpertheorie.
18—19 H. Wielandt, Tübingen, p-Sylowgruppen und p-Faktorgruppen.

Mittwoch, 28. Juni

9—11 P. Hall, Cambridge, Groups of automorphisms.
11—12 E. Witt, Hamburg, Automorphismen der Cayleyzahlen und Liesche Ringe.

Donnerstag, 29. Juni

10—12 P. Hall, Cambridge, Construction of soluble groups.
17—18 B. van der Waerden, Leipzig, Bericht über die Fittingsche Arbeit: Beiträge zur Theorie der Gruppen endlicher Ordnung.
18—19 A. Scholz, Kiel, Erweiterung und Aufspaltung von Gruppen.

Freitag, 30. Juni

10—11 W. Krull, Bonn, Primäre unendliche abelsche Gruppen.
11—12 W. Specht, Breslau, Darstellungstheorie endlicher Gruppen.

Die Vortragenden haben sich in dankenswerter Weise bereit erklärt, ihre Vorträge zur gemeinsamen Veröffentlichung in diesem Journal zur Verfügung zu stellen. Wir bringen diese Vorträge in dem vorliegenden Heft, und zwar die neuen und noch nicht veröffentlichten Forschungsergebnisse in vollständiger Form, und von den schon anderweitig veröffentlichten, sowie von zusammenfassenden Berichten kurze Auszüge. Das Heft gibt so ein vollständiges und in sich geschlossenes Bild der ganzen Veranstaltung.

Die Schriftleitung.

The classification of prime-power groups.

By *P. Hall* in Cambridge (England).

---

1. The problem of determining all the groups of a given order is an old one, which goes back right to the earliest days of group theory, and was, I believe, initiated by Cayley. It is about this problem as a central theme that I shall develop the remarks which follow.

In order to "determine", that is, to construct, all groups of a given kind, it is necessary first to know something of the structure of the groups in question. The methods of the various authors who have dealt with this *construction problem* differ principally in the extent and nature of the *structure theorems* to which they make appeal. Obviously, the more one knows of the structure of a given class of groups, the easier (*ceteris paribus*) it should be to construct them. For instance, nearly everyone who has made determinations of prime-power groups has used the fact that in such a group there always exist subgroups whose index is a prime number, and that all such subgroups are self-conjugate. This fact ensures that every group G of order p^n (p a prime) can be obtained in at least one way by a simple extension of some group G' of order p^{n-1}:

$$G = \{G', \xi\}, \quad \text{with} \quad \xi^{-1} G' \xi = G' \text{ and } \xi^p \text{ in } G'.$$

That G can in general be obtained by this method in many different ways is a very serious difficulty. A dictum of W. Magnus is here very much to the point. He writes [1]: Die Hauptschwierigkeit besteht dabei nicht in einer Konstruktion aller Gruppen eines bestimmten Typs, sondern in der Angabe eines vollständigen Systems nicht isomorpher Gruppen aus den konstruierten Gruppen.

Suppose that our problem is to determine all the groups of order $p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_r^{\alpha_r}$ where $p_1, p_2, \ldots, p_r$ are different primes and $\alpha_1 \geqq \alpha_2 \geqq \cdots \geqq \alpha_r$. It was observed by Otto Hölder, to whom we owe several most important contributions to this subject, that the degree of difficulty of this problem depends in the main on the size of the numbers α_i; the nature of the primes p_i makes as a general rule comparatively little difference. In particular, Hölder found that, if all the α_i are equal to 1, then even the number of prime factors r has little effect. All groups of square-free order are, according to Hölder, built up on the same general plan, which is a very simple one. For all such groups may be generated by two suitably chosen elements, α and β, which satisfy relations of the following form:

$$\alpha^m = \beta^n = 1, \quad \alpha^{-1} \beta \alpha = \beta^k,$$
$$(m, n) = 1, \quad \mu(mn) \neq 0, \quad k^m \equiv 1 \pmod{n}.$$

If we allow the numbers m, n and k to vary suitably, this system of formulae will define in turn every group of square-free order.

---

[1]) Cf. W. Magnus, Neuere Ergebnisse über auflösbare Gruppen, Jahresber. D. M. V. **47** (1937), 69.

If, to pass to the opposite extreme, the prime factors of the group order are not all different but all equal, we have quite another situation. To put it crudely, there is no apparent limit to the complication of a prime-power group. As we pass from the groups of order p^3 to those of order p^4, then to those of order p^5, and so on, at each step new structural phenomena make their appearance. And it seems unlikely that it will be possible to compass the overwhelming variety of prime-power groups within the bounds of a single finite system of formulae.

It is for this reason that those authors who have constructed prime-power groups on an extensive scale have found it necessary as a preliminary to split the problem up by introducing some system of classification. Thus Bagnera, who was the first to determine all the groups of order p^5 when p is an odd prime, made use of certain numerical invariants, notably, the number of independent generators and the number of inner automorphisms, and also of the presence or absence of an Abelian subgroup of index p. Schreier, in his well-known paper on the same subject, employs the fact that the commutator subgroup H of a group G of order p^5 is necessarily Abelian, and classifies these groups (implicitly) according to the type invariants of the Abelian groups H and G/H. And other authors, of whom G. A. Miller and H. R. Brahana are the most notable in this field, have used yet other methods of classification.

These methods, admirable as they are for the purpose for which they were devised, would clearly need to be supplemented, as one passed to groups of higher and higher orders, owing to the gradually increasing complexity of the groups concerned, if equally successful results were to be obtained. And it is natural to ask whether it would not be possible to introduce a system of classification which would apply without modification to all groups of prime-power order.

It is a *systematic* classification theory of this sort which will be developed in the present article. This theory has grown out of discussions which I have had over a considerable period with Mr. J. K. Senior of Chicago, to whom I should like to take this opportunity of expressing my deep indebtedness. It is our intention to publish a more detailed account of our results elsewhere, bearing particularly on the groups of order a power of 2.

2. So far as prime-power groups are concerned, it will probably be agreed that the most important number associated with the group, after the order, is the *class* of the group. This is defined as follows. It is a fundamental theorem that the central $Z_1 = Z_1(G)$ of a prime-power group G contains more than one element: $Z_1 > 1$. Applying this theorem to quotient groups, we see that, if $Z_i = Z_i(G)$ is defined (for $i > 1$) by the rule that Z_i/Z_{i-1} is the central of G/Z_{i-1}, then the series of characteristic subgroups Z_i of G must terminate after a certain number of terms in G itself. If $Z_{c-1} < Z_c = G$, then c is the class of G. A group of class 1 is an Abelian group and conversely. Z_i is sometimes referred to as the *i-th central* of G, and the series of centrals is the *upper central series* of G (aufsteigende Zentralreihe).

The class of a prime-power group may be defined in another way, the "dual" of this [2]). Let H and K be subgroups of G. Then by $[H, K]$ is denoted the subgroup generated by all the commutators,

$$[x, y] = x^{-1} y^{-1} xy,$$

of an element x of H with an element y of K. In particular, $[G, G]$ is the *commutator subgroup* of G. Writing $G = H_1$, and defining $[H_i, G] = H_{i+1}$, we have, in the case of

[2]) This duality has been remarked most notably by Prof. A. Speiser in his well-known book.

a prime-power group G,

$$G = H_1 > H_2 > H_3 > \cdots.$$

Thus the series of characteristic subgroups H_i must terminate in 1. It is easy to show that $H_c > H_{c+1} = 1$, if c is the class of G. The series of subgroups H_i is the *lower central series* of G (absteigende Zentralreihe).

The class provides an excellent classification of the groups of order p^4. These fall neatly into (a) the five Abelian groups of class 1, (b) six groups of class 2, and (c) either three or four groups of class 3, according to whether p is even or odd. But for higher powers of p as order, the classification by class is inadequate. For there seems to be no limit to the complexity even of the groups of class 2.

It might be thought that the introduction of a whole series of suitably chosen numerical invariants would meet this difficulty. And to some extent no doubt this is true. For example, one of the most useful and interesting series of invariants may be defined as follows. Let q_i denote the number of classes of conjugate elements of the p-group G which contain precisely p^i members. Since every class of conjugates has as the number of its elements a power of p, it follows that

$$q_0 + q_1 p + q_2 p^2 + \cdots$$

is the order of G. A somewhat analogous series of numbers may be obtained from a consideration of the (absolutely) irreducible representations of G. If r_i denotes the number of classes of equivalent irreducible representations of G which are of degree exactly p^i, then a known theorem of representation theory tells us that

$$r_0 + r_1 p^2 + r_2 p^4 + \cdots$$

is also equal to the order of G. Note that q_0 is the order of the central Z_1, and r_0 is the index of the commutator subgroup H_2.

The invariants q_i and r_i give a "good" classification, especially when taken in conjunction with the class of a group, at least as far as groups of order p^5. And by "good", I mean here a classification which is on the whole confirmed rather than contradicted by a more detailed examination of the properties of individual groups. But they have an important drawback. It is conceivable, namely, that two groups might have the same invariants q_i and r_i as it were by a sort of accident, without being at all closely related in structure. This does in fact happen among the groups of order 128. And this is a defect which is probably inherent in any system of classification which is based purely on numerical invariants. By using a sufficient number of invariants, the difficulty could doubtless be avoided for the groups of any given order. But one could never be certain of avoiding it completely.

For these reasons, we have preferred to adopt an entirely different principle of classification, of a directly structural character. This principle is based on two ideas. First, two groups G and G' are considered to be the same in the abstract sense if they can be placed in the relation of isomorphism to one another: $G \cong G'$. Clearly then, if we replace the relation of isomorphism by some weaker equivalence relation, $G \sim G'$, we shall obtain a classification of all groups into mutually exclusive classes. The second idea is that the Abelian groups, at least those of finite order, do not need to be classified, since they may be regarded as completely known. Thus we shall choose the relation $G \sim G'$ in such a way that the statement

$$G \sim 1$$

means the same as: G is Abelian. For this reason, we call the equivalence relation $\sim$, on which the system of classification is based, *isoclinism*; and read the relation

$$G \sim G'$$

as saying that G and G' are *isoclinic* groups. (The word isoclinic might perhaps be translated: gleich schief.)

Before giving the precise definition of these terms, it will be necessary to make a remark about commutators.

The characteristic property of Abelian groups, the permutability of their elements, may be expressed by saying that in an Abelian group the *commutator function* $[x, y]$ *is identically equal to* 1. Given any group G, which need not be of prime-power or even of finite order, the commutator function associates with each ordered pair of elements a, b of G the element $a^{-1}b^{-1}ab$ as its "value" for the argument-pair $x = a$, $y = b$. These values $[a, b]$ generate the commutator subgroup $H_2(G)$. But

$$[a, b] = [a\alpha, b\beta]$$

identically for all a, b of G, provided only that α and β belong to the central $Z_1(G)$. In other words, the value $[a, b]$ depends only on the pair of cosets of Z_1 to which a and b respectively belong. So that we may best regard the commutator as a function whose two arguments range over G/Z_1 rather than over G itself.

We are now in a position to state precisely the conditions under which two given groups G and G' are regarded as isoclinic. These conditions are three in number. Denoting by Z_1' and H_2' the central and commutator subgroup of G', they are:

(1) $G/Z_1 \cong G'/Z_1'$;

(2) $H_2 \cong H_2'$;

(3) it shall be possible to choose the isomorphisms (1) and (2) in such a way that whenever, under (1), the elements Z_1a and Z_1b of G/Z_1 correspond respectively to the elements $Z_1'a'$ and $Z_1'b'$ of G'/Z_1', then, under (2), the element $[a, b]$ of H_2 shall correspond to the element $[a', b']$ of H_2'.

When this is the case, we may say that the isomorphism (2) is *induced by* the isomorphism (1). It is quite possible for two groups to have isomorphic central quotient groups and isomorphic commutator subgroups without being isoclinic, for it may not be possible to choose the isomorphisms (1) and (2) to satisfy the consistency condition (3). Roughly, the definition amounts to this, that two groups are isoclinic if and only if their commutator functions are essentially the same, viz. if they have the same range of arguments (1), the same range of values (2), and the same correspondence of values with arguments (3).

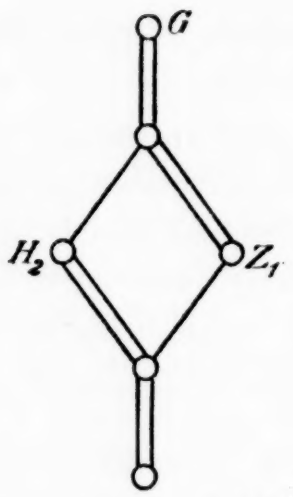
By an *isoclinism* between two groups is meant any isomorphism (1) between their central quotients which induces, in the sense of (3), a corresponding isomorphism between their commutator subgroups.

It is clear that $G \sim 1$ if and only if G is Abelian. And it is equally clear that the relation of isoclinism is, in fact, an equivalence relation. In respect of it, all groups fall into a number of mutually exclusive *families*, two groups belonging to the same family if and only if they are isoclinic.

3. I propose now to trace in brief outline some of the consequences of the definition of isoclinic groups which has just been given.

Any quantity depending on a variable group and which is the same for any two groups of the same family will be called a *family invariant*. Thus, if we do not distinguish between isomorphic groups, we may say that the commutator subgroup and the central quotient group are family invariants. On the other hand, as the Abelian family shows, the central and the commutator quotient group are not family invariants. This is made

clear in the accompanying diagram, where the double lines denote factors which are family invariants.



An isoclinism between two groups G and G' of the same family induces an isomorphism between their commutator subgroups: $H_2 \cong H_2'$. It is important to remark that this is an operator-isomorphism, if we take as operators the inner automorphisms of the two groups and identify those pairs of inner automorphisms which correspond in the given isoclinism.

It follows from this operator-isomorphism that *the higher commutator subgroups*, such as those of the lower central series $H_3, H_4, \ldots$, and more complex types such as the series of successive derived groups $\Theta_1 = H_2, \Theta_2, \Theta_3, \ldots$, *are all family invariants.* As a corollary, the class of a prime-power group is a family invariant.

An isoclinism of G with G', being an isomorphism (of a certain kind) between G/Z_1 and G'/Z_1', establishes a (1, 1) correspondence between the subgroups of G which contain Z_1 on the one hand and the subgroups of G' which contain Z_1' on the other. It is easy to see that corresponding subgroups are isoclinic. Thus the assignment of these subgroups into families is independent of the particular groups G, G' and depends only on the family to which they belong.

With regard to subgroups which do not contain the central, we have the following rule. *The family to which any subgroup K of a group G belongs is the same as that which contains its join with the central of G:*

$$K \sim KZ_1(G).$$

A particularly important special case is that in which $KZ_1 = G$, i. e. in which K covers G/Z_1. In that case, K is isoclinic with G itself. But obviously the converse is also true, at least when G/Z_1 is of finite order. Thus *G is isoclinic with its subgroup K if and (for finite G/Z_1) only if $KZ_1 = G$.*

We turn next to consider the families of quotient groups. An isoclinism between G and G' induces, as we have seen, an operator-isomorphism between H_2 and H_2'. It follows that, if K is any self-conjugate subgroup of G contained in H_2, the corresponding subgroup K' of H_2' will be self-conjugate in G'; and it is easy to see that, in these circumstances, G/K is isoclinic with G'/K'. In other words, we have a (1, 1) correspondence between quotient groups G/K for which K lies in H_2, and quotient groups G'/K' for which K' lies in H_2', and corresponding quotient groups are of the same family.

With regard to quotient groups G/K for which K does not lie in H_2, we have the following rule. *The family to which any quotient group G/K of a group G belongs is the same as that which contains the quotient group of the meet of K with H_2:*

$$G/K \sim G/(K \wedge H_2).$$

A particularly important special case is that in which $K \wedge H_2 = 1$, i. e. in which K avoids H_2. In that case, G/K is isoclinic with G itself. But obviously the converse is

true, at least when H_2 is of finite order. Thus G *is isoclinic with its quotient group* G/K *if and* (*for finite* H_2) *only if* $K \wedge H_2 = 1$.

There is a simple rule for the families of direct products. If $G_1 \sim G_1'$ and $G_2 \sim G_2'$, then $G_1 \times G_2 \sim G_1' \times G_2'$. In particular, if A is Abelian, i. e. if $A \sim 1$, we have $G \sim G \times A$ for all G.

For certain types of groups G the converse of this last statement is true, viz. every group G' which is isoclinic with G is isomorphic with the direct product of G and an Abelian group. This is the case, for example, if G coincides with its commutator subgroup and if at the same time the central of G is 1. Thus, for groups of this kind, our classification leads only to trivialities. And it is desirable, therefore, to remark that although the classification applies formally to all groups whatsoever, its real interest lies in its application to prime-power groups. In a prime-power group, we always have $Z_1 > 1$ and $H_2 < G$. Thus the question whether two prime-power groups are of the same family or not depends on relations between groups of smaller prime-power order. This gives the classification of prime-power groups a certain character of recurrence.

To return to the general case, I shall now prove the theorem that *in every family there exist groups for which* $Z_1 \leqq H_2$.

Let G be any group and let $\xi_1, \xi_2, \ldots$ be a set of elements which generate G. Let A be the free Abelian group generated by $\eta_1, \eta_2, \ldots$. Then $G \sim G \times A$. Let G' denote the subgroup of $G \times A$ which is generated by $\xi_1\eta_1, \xi_2\eta_2, \ldots$. Clearly $G'A$ coincides with $G \times A$, and since A is contained in the central of this group it follows that $G' \sim G \times A$, by a rule already explained. Thus $G' \sim G$. The commutator quotient group G'/H_2' is isomorphic with A. Also,

$$Z_1'/(Z_1' \wedge H_2') \cong Z_1'H_2'/H_2'.$$

Thus the quotient group of $Z_1' \wedge H_2'$ in Z_1' is isomorphic with a subgroup of the free Abelian group G'/H_2'. Hence it is itself either 1 or a free Abelian group. In either case, Z_1' is the direct product of $Z_1' \wedge H_2'$ with another group K'. Since $K' \wedge H_2' = 1$, we have $G'/K' \sim G'$, by a rule mentioned before. But the central of G'/K' is clearly Z_1'/K' and this is contained in the commutator subgroup of G'/K' which is $K'H_2'/K'$. Thus G'/K', which is isoclinic with G, has the required property.

All the groups of a given family which have this property that $Z_1 \leqq H_2$ are said to form the *stem* of the family, and will be called *stem groups*. It is clear that all stem groups of a given family have the same order; if G is any group of the family, the order of the stem groups is

$$(G:Z_1) \cdot (Z_1 \wedge H_2:1) = (G:Z_1H_2) \cdot (H_2:1).$$

Furthermore, in the case of groups of finite order, *the stem of a family may be defined to consist precisely of all groups of the family which are of minimal order*, i. e. all groups whose order is not greater than that of any other isoclinic group.

By a *branch* of a given family will be meant the system of all groups of that family which have a given order. Since the order of a group G is equal to the order of an isoclinic stem group, multiplied by the factor

$$(Z_1:Z_1 \wedge H_2) = (Z_1H_2:H_2),$$

this factor will be called *the branch factor* for the group G. The stem is the branch having the branch factor equal to 1.

The notion of branch factor is convenient for the discussion of the behaviour of the numerical invariants q_i and r_i. For we have the theorem that, if G and G' are isoclinic prime-power groups, the invariants q_i and r_i of G bear to the corresponding in-

variants q_i' and r_i' of G' a constant ratio, which is equal to the ratio of the branch factor of G to that of G', or what is the same, the ratio of the orders of G and G'. Thus two isoclinic stem groups have the same set of invariants q_i and r_i, and we obtain the corresponding invariants for any group G of the family by multiplying each stem invariant by the branch factor of G. Thus the determination of the stem invariants gives us implicitly the values of the q's and r's for all groups of the family.

These results are not restricted to prime-power groups. We may say quite generally that the number of classes of conjugate elements which contain just k members each is the the same for any two isoclinic groups of the same finite order, as is also the number of classes of equivalent absolutely irreducible representations of degree exactly d. And the ratio of these numbers to the corresponding numbers for a stem group of the same family is equal to the branch factor in every case.

I ought also to remark that the result only holds for the case of absolutely irreducible representations, and not, in general, for representations irreducible in a field which is not algebraically closed. For example, the simplest family of non-Abelian groups is that which contains the quaternion group and the dihedral group of order 8. These two groups constitute the stem of this family. But it is well-known that the dihedral group has an irreducible representation of degree 2 with real coefficients, while the quaternion group has not.

4. The main interest of a theory such as has just been outlined must lie, I think, in its detailed application to the actual classification of prime-power groups. Only in this way can we discover exactly the extent to which it is capable of introducing order and coherence among the vast array of individual results which lie to hand. In the following, it will not be possible to do more than illustrate, by means of a few examples, the usefulness of the notion of isoclinism in the study of the comparative anatomy of these groups. The examples I have chosen are

(a) the classification of the groups of order p^5, $p > 3$;

(b) the classification of the p-groups having an Abelian subgroup of index p.

If the stem groups of a family are prime-power groups of order p^ϱ, the number ϱ will be called the *rank* of the family. Thus the Abelian groups form a family of rank 0. Among the groups of order p^5 will occur representatives from all families of rank 5 or less. The number of these families is 8 for $p = 2$ and 10 for $p > 2$. The classification is completely parallel for all values of $p > 3$, but there are certain very minor differences when $p = 3$. For the sake of simplicity, therefore, let $p > 3$. The determination of the 10 families in question may be regarded as a first step in the determination of the individual groups of order p^5. Once the families have been obtained, the construction of the individual groups is a comparatively simple matter.

In determining the families, we may confine our attention to stem groups. It is natural, therefore, to proceed in order of increasing rank. Clearly there are no families of rank 1 or 2, for all groups of order p and p^2 are Abelian. The two non-Abelian groups of order p^3 form the stem of a family Φ_2 whose members are characterised by either of the following two properties:

I. their central is of index p^2,

II. they have more than one Abelian subgroup of index p, without themselves being Abelian. It is easy to see that any two groups with either of these properties must be isoclinic.

Among the groups of order p^4, beside the 5 Abelian groups and the 6 groups of the family Φ_2, there are 4 others, forming the stem of a family Φ_3 of groups of class 3. The

groups of this family are characterised by the property that they all have an Abelian subgroup of index p and in addition H_2 is of order p^2, H_3 of order p. They can also be characterised in other ways. For example, by the property that G/Z_1 is the non-Abelian group of order p^3 whose elements are all of order p and at the same time $H_2 \wedge Z_1$ is of order p.

Before passing to the families of rank 5, it will be convenient to consider more generally the relations which may hold between the families of groups which have a given group K of inner automorphisms. Given a group K, the problem of constructing groups G of which K is the homomorphic image modulo some self-conjugate subgroup of the central of G is one which has been frequently studied. Such a G has a self-conjugate subgroup L which is such that

$$G/L \cong K \quad \text{and} \quad L \leqq Z_1(G).$$

Problems of this kind arise particularly in connection with the representation of a given group of finite order by fractional linear substitutions, and important contributions have been made, notably by I. Schur, A. Speiser and R. Brauer. From our present point of view, we are concerned exclusively with the case in which $L = Z_1(G)$. And for inappropriate choices of K, the problem of constructing G may then be impossible, for not every group can be the group of inner automorphisms of another group.

The question of what conditions a group K must fulfil in order that it may be the central quotient group of another group G,

$$K \cong G/Z_1,$$

is an interesting one. But while it is easy to write down a number of necessary conditions, it is not so easy to be sure that they are sufficient. Suppose that α is an element of K, different from 1; and let J_α denote the subgroup of K generated by all elements ξ such that some power of ξ is equal to α. If, for some choice of α in K, we can arrange that $J_\alpha = K$, then it is clear that in any group G for which

$$G/L \cong K, \quad L \leqq Z_1(G),$$

the coset of L which corresponds to the element α of K must belong to the central of G; and therefore, α being by hypothesis different from 1, we should have $Z_1(G) > L$. Thus, if $J_\alpha = K$, K cannot be a group of inner automorphisms.

This rule can be applied in a very simple manner to the case in which K is a p-group of order p^n, at any rate when the class of K is less than p. For it is known that such a K has a definite *type*, which is a partition of n having much the same significance as in the familiar case of an Abelian prime-power group. If now the two largest parts of this partition, i. e. the two largest type-invariants, are different, say μ_1 and μ_2, where $\mu_1 > \mu_2$, then K has an element ξ of order p^{μ_1}; and if we put $\alpha = \xi^{p^{\mu_1 - 1}}$, it is known that $\eta^{p^{\mu_1 - 1}}$ is also equal to α for every element η of K which can be obtained from ξ by multiplication with an element of order p^{μ_2} or less. And these elements η generate K. Hence, *if the class of K is less than p, K can only be a group of inner automorphisms if its two largest type-invariants are the same.*

When the class of K exceeds p, we have no such simple rule of exclusion. The case of practical interest is when $p = 2$. It is quite easy to calculate the subgroups J_α directly, if K is not too large. But experience shows that the condition that all the J_α must be proper subgroups of K if K is to be a group of inner automorphisms is not a sufficient one. The simplest *Gegenbeispiel* is a certain group of order 32, which can be excluded on the following ground. Let the element α of K be expressed as a product

$$\alpha = \beta\gamma \cdots \varepsilon. \tag{1}$$

For every such expression, adjoin to J_α the meet of the subgroups $J_\beta, J_\gamma, \ldots, J_\varepsilon$. If, in this way, by a suitable choice of $\alpha \neq 1$, and of expressions (1), we can extend J_α until after a certain number of adjunctions we arrive at the whole group K, then K cannot be a group of inner automorphisms. I do not know whether this more elaborate rule gives a sufficient condition or not. In any case, this difficulty is not serious for groups of order p^5, $p > 3$, for the rule about the type-invariants gives then not only a necessary but also sufficient condition.

To return to the relations between groups which have the same central quotient groups, many results bearing on this question are to be found in a valuable paper by I. Schur [3]). For the restricted purposes of the classification theory, however, it is possible that some of Schur's proofs may be simplified. As an example, we shall prove an important theorem of Schur from our present point of view.

Let G and G' be any two groups such that

$$G/Z_1 \cong G'/Z_1' \cong K.$$

Let $\varkappa_1, \ldots, \varkappa_r$ be any system of generators of K, let $Z_1\xi_1, \ldots, Z_1\xi_r$ be the corresponding cosets of Z_1, and $Z_1'\xi_1', \ldots, Z_1'\xi_r'$ those of Z_1'. Further let $\eta_1, \ldots, \eta_r$ generate the free group F with r generators. If $\bar{G}$ and $\bar{G}'$ are the subgroups of G and G' generated respectively by the ξ's and the ξ''s, then $G = \bar{G}Z_1$, $G' = \bar{G}'Z_1'$, so that

$$G \sim \bar{G}, \quad G' \sim \bar{G}'.$$

If now we make each generator η_i of F correspond successively with $\varkappa_i$, with ξ_i, and with ξ_i', we obtain the three groups K, $\bar{G}$ and $\bar{G}'$ as homomorphic images of F:

$$K \cong F/N, \quad \bar{G} \cong F/L, \quad \bar{G}' \cong F/L';$$

the significance of N, L, L' is well-known. Moreover, L and L' are both contained in N and are such that N/L belongs to the central of F/L, and N/L' to the central of F/L'.

If therefore we put $M = [F, N]$, both L and L' must contain M, and hence the central of F/M is necessarily equal to N/M, so that F/M also has K as its group of inner automorphisms. Moreover both $\bar{G}$ and $\bar{G}'$ are quotient groups of F/M.

Now the group F/M depends only on the particular system of generators chosen for K, and not at all on G or G'. We conclude then that *every group G such that $G/Z_1 = K$ is isoclinic with some quotient group of the fixed group F/M, which also has its central quotient isomorphic with K.* Thus the family Φ to which F/M belongs has the following maximal property: if G belongs to Φ, then $G/Z_1 \cong K$, and on the other hand if $G/Z_1 \simeq K$, then every group of the family Φ has a quotient group which is isoclinic with G. For this reason, we may call Φ the *maximal family* for the given group of inner automorphisms K. It is independent of the choice of the generators $\varkappa_i$ of K and depends on K alone. If K is of finite order, then it is not difficult to show that the commutator subgroup of a group of Φ is also of finite order. Thus the stem groups of Φ are finite groups. From such a stem group, we shall therefore be able to obtain representative stem groups for all the other families (if there are any) having K as group of inner automorphisms.

The construction of a stem group of the maximal family is thus seen to be the key to the determination of all families of groups G with given G/Z_1. This method may be applied in particular to the families of prime-power groups of rank 5. The central quotient group must here be either of order p^3 or of order p^4. Only two groups of order p^3

---

[3]) I. Schur, Über die Darstellung der endlichen Gruppen durch gebrochene lineare Substitutionen, Crelle **127** (1904), 20—50; see also *ibid.* **132** (1907), 85—137.

are relevant, viz. those whose type-invariants are all equal to 1. If K is the Abelian group of type (1^3), a stem group of the maximal family can be written down at once, viz. the group defined by the relations

$$\alpha_1^p = \alpha_2^p = \alpha_3^p = \gamma_{12}^p = \gamma_{23}^p = \gamma_{31}^p = 1,$$

where $\gamma_{ij} = [\alpha_i, \alpha_j]$, and it is understood that the γ_{ij} belong to the central of the group. This group is of order p^6, so that the maximal family is of rank 6. We may pass to a quotient group of order p^5 by putting e. g. $\gamma_{12} = 1$. The $1 + p + p^2$ such quotient groups are all isoclinic, so that we obtain only a single family Φ_4 of rank 5 having the given Abelian group as central quotient group.

If next we take for K the (unique) non-Abelian group of type (1^3), we find without difficulty that the rank of the maximal family cannot exceed 5. The group defined by

$$\alpha_1^p = \alpha_2^p = \alpha_3^p = \gamma_{13}^p = \gamma_{23}^p = 1, \quad \alpha_3 = \gamma_{12},$$

with γ_{13} and γ_{23} in the central, is in fact of order p^5, and has its central quotient of order p^3 and non-Abelian. This gives the only relevant family of rank 5, and may be denoted by Φ_6.

Passing next to the families with central quotient K of order p^4. First suppose that K is Abelian. Only two types are possible, (2^2) and (1^4). It is clear that the maximal family for the former is of rank 6, a stem group being defined by

$$\alpha_1^{p^2} = \alpha_2^{p^2} = \gamma_{12}^{p^2} = 1,$$

with γ_{12} in the central. There is only one quotient group to consider; it is obtained by putting $\gamma_{12}^p = 1$. But the central quotient of this group is not of order p^4. Indeed it belongs to the family Φ_2 of rank 3. So there is no family of rank 5 having its central quotient groups isomorphic with the Abelian group of type (2^2), a result easy to verify directly.

The case in which K is the elementary Abelian group of order p^4 is very different. Here the maximal family is of rank 10, and it might be supposed that the discussion of the quotient groups of order p^5 of a group of order p^{10} would be somewhat tedious. If however we regard K as a linear space L_4 with integers mod p as coefficients, we may then picture the commutator subgroup (or central) of a stem group of the maximal family as the carrier space L_6 of the Grassmannian which represents the L_2's of L_4. The subspaces L_5 of L_6, which give rise to the quotient groups of order p^5 which are in question, will then correspond to linear complexes of L_2's in L_4. And there are two types of these only, the special and the general. It is easy to see that a special complex will correspond to a quotient group of family Φ_2 which is irrelevant to our purpose. While a general complex will give rise to a quotient group which in fact does have K as its group of inner automorphisms. It is not difficult to show that there are precisely two distinct types of such quotient groups of order p^5, which are isoclinic, and constitute the stem of a family Φ_5 of rank 5.

We may remark in passing that the families of p-groups having H_2 of order p are necessarily of odd rank $r = 2k + 1$, and that there is just one such family for each value of $k = 1, 2, \ldots$. Φ_2 and Φ_5 are the cases $k = 1, 2$. The stem of these families always consists of two groups, one of type (1^{2k+1}), the other of type $(1^{2k-1}\ 2)$.

Consider next more briefly the families of rank 5 for which K is of order p^4 and non-Abelian. There are only three possibilities for K.

(a) If K is the group of family Φ_2 and type (2^2), then the maximal family Φ_8 is itself of rank 5, and so there are no others.

(b) If K is the group of family Φ_2 and type (1^4), the maximal family is of rank 8. A detailed discussion shows that there are 3 distinct families of rank 7 with this group K as group of inner automorpisms, as well as 6 distinct families of rank 6, but only one family Φ_7 of rank 5.

(c) If K is the group of family Φ_3 and type (1^4), the maximal family is of rank 6, and gives rise to two distinct families of rank 5, Φ_9 and Φ_{10}, which are easy to distinguish owing to the fact that the groups of the former have an Abelian subgroup of index p, while those of the latter have not.

Since all other possibilities for K are excluded by the rule about type-invariants, the classification of the groups of order p^5 into families is complete. A short table of the principal family invariants of these ten families will give at a glance a complete view of the main structural features which a group of order p^5 can exhibit.

Turning finally to the p-groups which possess Abelian subgroups of index p, these form a natural category of groups which have been frequently investigated. Their classification into families is particularly simple. Let G be any one of these groups, and let A be an Abelian subgroup of index p, so that $G = \{A, \xi\}$, where ξ^p lies in A. If α and β are two elements of A, then

$$[\alpha\beta, \xi] = [\alpha, \xi] \cdot [\beta, \xi].$$

It follows that if we make every element α of A correspond to the element $[\alpha, \xi]$, which is also in A, we obtain an endomorphism of the Abelian group A. I will denote this endomorphism by θ, and write

$$[\alpha, \xi] = \alpha^\theta.$$

From the fact that ξ^p lies in A, we deduce that

$$\psi = p\theta + \binom{p}{2}\theta^2 + \cdots + \theta^p$$

is the zero endomorphism of A, which maps every element of A on to 1.

For every α of A, there exists an integer k such that $\alpha^{\theta^k} = 1$. The least such k will be called the *θ-exponent* of α. The elements whose θ-exponent is equal to k all belong to Z_k but not to Z_{k-1}. Dually, I will call l the *θ-power* of α if there exists an element β of A such that $\beta^{\theta^l} = \alpha$, but no element of A whose θ^{l+1}-th power is equal to α. The elements whose θ-power is equal to l all belong to H_{l+1} but not to H_{l+2}.

Now suppose that G is a stem group, and let the order of its commutator subgroup H_2 be p^n. We may associate with the group G a certain partition of the number n, in the following way. If the order of H_2/H_3 is p^{λ_1}, that of H_3/H_4 is p^{λ_2}, and so on, then clearly

$$\lambda_1 + \lambda_2 + \cdots = n.$$

If α is an element whose θ-power is equal to l, and $l \geqq 2$, then α belongs to H_{l+1} but not to H_{l+2}, and there exists an element β of A such that

$$\beta^\theta = \alpha.$$

It follows that $\alpha^p = \beta^{p\theta}$ is congruent to $\beta^\psi = 1 \bmod H_{l+2}$, since $\alpha^\theta, \alpha^{\theta^2}, \ldots$ all have θ-powers greater than l. Thus the factor groups H_i/H_{i+1} $(i > 1)$ are all elementary Abelian groups.

Consider particularly H_2/H_3, and let us intersect it with the terms of the upper central series. Write

$$Z_i H_3 \wedge H_2 = K_i.$$

Thus, for some value of r,

$$H_3 = K_0 \leqq K_1 \leqq K_2 \leqq \cdots \leqq K_r = H_2.$$

If $(K_i : K_{i-1}) = p^{\mu_i}$, we may chose μ_i elements

$$\alpha_{i,1}, \alpha_{i,2}, \ldots, \alpha_{i,\mu_i}$$

which generate K_i mod K_{i-1}. Clearly, we must have

$$\mu_1 + \mu_2 + \cdots + \mu_r = \lambda_1.$$

Moreover the least self-conjugate subgroup of G which contains the λ_1 elements $\alpha_{i,j}$ is, by an elementary property of the lower central series, equal precisely to H_2. It is obvious therefore that every element of H_2 can be expressed in the form

$$(1) \qquad \Pi \alpha_{ij}^{f_{ij}(\theta)},$$

where $f_{ij}(\theta)$ is a polynomial in θ with integer coefficients, and of degree at most equal to $i-1$. But the form of the zero operator shows that we can even suppose the coefficients to be the numbers $0, 1, \ldots, p-1$. Finally, if this further restriction is made, it can be shown that the form (1) is unique. Since there are now just p^i possibilities for the polynomial $f_{ij}(\theta)$, we deduce that

$$\mu_1 + 2\mu_2 + 3\mu_3 + \cdots = n.$$

And it is an easy further step to prove that the partition

$$(1^{\mu_1} 2^{\mu_2} \ldots)$$

is the "associate" of that whose parts are $\lambda_1, \lambda_2, \ldots$. Furthermore the type-invariants of the Abelian group H_2 may now be written down. If we put

$$\begin{aligned}
v_1 &= \mu_1 + 2\mu_2 + 3\mu_3 + \cdots + (p-1)(\mu_{p-1} + \mu_p + \mu_{p+1} + \cdots), \\
v_2 &= \mu_p + 2\mu_{p+1} + 3\mu_{p+2} + \cdots + (p-1)(\mu_{2p-2} + \mu_{2p-1} + \mu_{2p} + \cdots), \\
v_3 &= \mu_{2p-1} + 2\mu_{2p} + 3\mu_{2p+1} + \cdots + (p-1)(\mu_{3p-3} + \mu_{3p-2} + \cdots),
\end{aligned}$$

and so on, then the partition whose parts are $v_1, v_2, \ldots$ is the associate of the type-partition of H_2. In particular, if $p = 2$, we have $v_i = \lambda_i$ for each value of i, so that H_2 is of type $(1^{\mu_1} 2^{\mu_2} \cdots)$. In every case, however, this partition $(1^{\mu_1} 2^{\mu_2} \cdots)$, or alternatively the associated partition formed by the λ's, determines the nature of H_2. But it also determines uniquely the group G/Z_1, and it can indeed be proved that any two stem groups G and G', having each an Abelian subgroup of index p, are isoclinic if and only if their commutator subgroups are of the same order p^n and if in addition they determine the same partition $(1^{\mu_1} 2^{\mu_2} \cdots)$ of n. Thus (*for the p-groups which have Abelian subgroups of index p*) *there is a* (1, 1) *correspondence between partitions and families.* In all these families, the rank is $n + \lambda_1 + 1$.

The families of this kind which have been mentioned previously are Φ_2, Φ_3, Φ_4 and Φ_9. They correspond respectively to the partitions (1), (2), (1^2) and (3).

Eingegangen 1. Juli 1939.

Über Gruppen und zugeordnete Liesche Ringe.

Von *Wilhelm Magnus* in Berlin.

1. W. B. Fite[1]) hat im Jahre 1906 bei seinen Untersuchungen über Gruppen von Primzahlpotenzordnung folgende charakteristische Untergruppen einer gegebenen Gruppe $\mathfrak{G}$ eingeführt: Ist $\mathfrak{H}$ eine Untergruppe von $\mathfrak{G}$, so verstehe man unter $[\mathfrak{H}, \mathfrak{G}]$ die von allen Kommutatoren eines beliebigen Elementes von $\mathfrak{G}$ mit einem beliebigen Element von $\mathfrak{H}$ erzeugte Untergruppe von $\mathfrak{G}$, und man definiere rekursiv: $\mathfrak{G}_n = [\mathfrak{G}_{n-1}, \mathfrak{G}]$ $(n = 2, 3, \ldots)$; $\mathfrak{G}_1 = \mathfrak{G}$. Die Gruppen $\mathfrak{G}_n$ $(n = 1, 2, \ldots)$ heißen nach P. Hall[2]) die „Gruppen der unteren Zentralreihe von $\mathfrak{G}$"; die Untersuchungen von Reidemeister[3]) und von Hall haben gezeigt, daß sie ein außerordentlich anwendungsfähiges Instrument in der allgemeinen Gruppentheorie bilden. Im folgenden soll vor allem die Beziehung der Gruppen $\mathfrak{G}_n$ zu einem der Gruppe $\mathfrak{G}$ zugeordneten Lieschen Ring nebst einigen einfachen Anwendungen dieser Zuordnung dargelegt werden.

2. Die Gruppen $\mathfrak{G}_n/\mathfrak{G}_{n+1}$ sollen mit $\mathfrak{A}_n(\mathfrak{G})$, oder, wenn keine Verwechslung möglich ist, mit $\mathfrak{A}_n$ bezeichnet werden. Wenn $\mathfrak{G}$ endlich viele Erzeugende besitzt, so besitzen die abelschen Gruppen $\mathfrak{A}_n$ eine endliche Basis. Es liegt nahe, solche Gruppen $\mathfrak{G}$ und $\mathfrak{G}^*$ zu einem Typ zusammenzufassen, für die für alle Werte von $n = 1, 2, \ldots$ stets die Gruppen $\mathfrak{A}_n(\mathfrak{G})$ und $\mathfrak{A}_n(\mathfrak{G}^*)$ isomorph sind. Hierbei ergibt sich dann die Frage, wann man zu einer vorgegebenen Folge von Abelschen Gruppen $\mathfrak{A}_1, \mathfrak{A}_2, \ldots$ eine Gruppe $\mathfrak{G}$ finden kann, so daß für $n = 1, 2, \ldots$ stets $\mathfrak{A}_n \simeq \mathfrak{A}_n(\mathfrak{G})$ ist. Es ist leicht zu sehen, daß die Gruppen $\mathfrak{A}_n$ hierbei nicht unabhängig voneinander wählbar sind; die zwischen ihnen bestehenden Beziehungen lassen sich nach der folgenden Methode untersuchen:

3. Man betrachte $\mathfrak{G}$ als Faktorgruppe $\mathfrak{F}/\mathfrak{R}$ einer freien Gruppe $\mathfrak{F}$ nach einem Normalteiler $\mathfrak{R}$. Es ist dann

$$\mathfrak{A}_n(\mathfrak{G}) \sim \mathfrak{F}_n/\{\mathfrak{F}_{n+1} \cdot (\mathfrak{F}_n, \mathfrak{R})\}, \tag{1}$$

wobei durch $\{\}$ das Produkt der in der Klammer stehenden Normalteiler bezeichnet wird. $\mathfrak{A}_n(\mathfrak{G})$ ist somit eine Faktorgruppe von $\mathfrak{A}_n(\mathfrak{F})$, und diese Gruppe soll nun zunächst untersucht werden. Man denke sich $\mathfrak{G}$ erzeugt aus gewissen Elementen $a, b, \ldots$; diese lassen sich zugleich als Erzeugende von $\mathfrak{F}$ ansehen, wobei zwischen den Erzeugenden von $\mathfrak{G}$ dann im allgemeinen mehr Relationen bestehen werden als zwischen denen von $\mathfrak{F}$. Nunmehr setze man

$$\begin{gathered} a = 1 + x, \quad b = 1 + y, \ldots \\ a^{-1} = 1 - x + x^2 \mp \cdots, \quad b^{-1} = 1 - y + y^2 \mp \cdots, \end{gathered} \tag{2}$$

[1]) W. B. Fite, Transactions of the American Mathematical Society **7**, 61—68, 1906.

[2]) P. Hall, Proceedings of the London Mathematical Society (2) **36**, 29—95, 1933.

[3]) K. Reidemeister, Abhandlungen aus dem mathematischen Seminar der Hamburgischen Universität **5**, 33—39, 1927.

wobei $x, y, \ldots$ erzeugende Elemente eines „freien" Ringes $\mathfrak{R}$ mit Einheitselement 1 seien; der Ring $\mathfrak{R}$ soll, genauer gesagt, aus allen formal verschiedenen Potenzreihen mit ganzzahligen Koeffizienten in den nicht kommutativen, aber assoziativen Variablen $x, y, \ldots$ bestehen [4]). Jedem „Wort" oder Potenzprodukt $W(a, b, \ldots)$ der Erzeugenden von $\mathfrak{F}$ ist dann ein Element von $\mathfrak{R}$ zugeordnet, das man sich nach Gliedern gleicher Dimension oder gleichen Grades in den Variablen $x, y, \ldots$ geordnet denken kann, d. h. es ist:

$$W(a, b, \ldots) = 1 + d_n(x, y, \ldots) + d_{n+1}(x, y, \ldots) + \cdots, \tag{3}$$

wobei $d_n(x, y, \ldots)$ die Glieder n-ten Grades bedeutet; die Glieder vom 1. bis $(n-1)$-ten Grade seien dabei identisch Null; zum Beispiel ist:

$$aba^{-1}b^{-1} = 1 + xy - yx + \cdots = 1 + (xy - yx)\sum_{\nu,\mu=0}^{\infty}(-1)^{\nu+\mu}x^{\nu}y^{\mu}.$$

In diesem Fall ist $n = 2$, $d_2 \equiv xy - yx$.

Es läßt sich nun zeigen [4b]), daß dann und nur dann in der Beziehung (3) gerade die Glieder 1. bis $(n-1)$-ten Grades identisch verschwinden, wenn W ein Element von $\mathfrak{F}_n$ aber nicht von $\mathfrak{F}_{n+1}$ ist; indem man dem Element $W(a, b, \ldots)$ das Polynom $D(W) \equiv d_n(x, y, \ldots)$ zuordnet, hat man jedem Element $\neq 1$ aus $\mathfrak{F}$ ein homogenes Polynom n-ten Grades in $x, y, \ldots$ zugeordnet, dessen Grad zugleich genau angibt, welches die erste Gruppe der unteren Zentralreihe von $\mathfrak{F}$ ist, die W enthält. Zweckmäßigerweise definiert man noch $D(1)=0$. Man bemerkt leicht, daß (für $D(W_1)+D(W_2) \neq 0$)

$$\begin{cases} D(W_1W_2) = D(W_1) + D(W_2), \text{ wenn } W_1, W_2 \text{ den gleichen Grad besitzen,} \\ D(W_1W_2) = D(W_1) \text{ wenn der Grad von } W_1 < \text{Grad von } W_2 \text{ ist.} \end{cases} \tag{4}$$

In jedem Falle gilt $D(W_1W_2) = D(W_2W_1)$. Mit Hilfe dieser Beziehung läßt sich leicht eine (nicht archimedische) Bewertung von $\mathfrak{F}$ erklären, und der Kern einiger Schlüsse, die bei der Verwendung der unteren Zentralreihe auftreten, gehört in die topologische Algebra.

Durch die hier angegebene Beziehung zwischen den Gruppen der unteren Zentralreihe und den „Entwicklungen" (3) der Elemente von $\mathfrak{F}$ in eine Potenzreihe aus $\mathfrak{R}$ lassen sich eine Reihe von gruppentheoretischen Sätzen beweisen. Man vergleiche hierzu [4c]). Weiterhin kann man beispielsweise die von P. Hall [2]) erwähnte Frage beantworten, ob es nicht-reguläre (im Hallschen Sinne) p-Gruppen gibt, für die die Ordnung der Automorphismengruppe die von Hall angegebene obere Schranke erreicht. Dies ist tatsächlich der Fall; man erhält solche Gruppen mit den Erzeugenden $a, b, \ldots$, indem man in (2) auf der rechten Seite für $x, y, \ldots$ Erzeugende eines Ringes $\mathfrak{R}^*$ einsetzt, der aus $\mathfrak{R}$ dadurch hervorgeht, daß man in $\mathfrak{R}$ die Relationen $px = 0$, $py = 0, \ldots$ ansetzt, und überdies alle Produkte von mindestens $m \geqq p$ Faktoren $x, y, \ldots$ gleich Null setzt. Auch die Ordnung einer solchen Gruppe läßt sich nach E. Witt [5]) bestimmen.

4. Es ist bemerkenswert, daß die Polynome $d_n(x, y, \ldots)$ nicht beliebige Polynome n-ten Grades sein können. Vielmehr gilt, daß sie sich als Bilder der Elemente eines Lieschen Ringes Λ bei einer geeigneten Darstellung von Λ durch Elemente von $\mathfrak{R}$ auffassen lassen. Ein Liescher Ring wird erklärt als eine Gesamtheit von Elementen $\varphi, \psi, \chi, \ldots$, zwischen denen eine Addition und eine Multiplikation erklärt ist, wobei statt des kommutativen und assoziativen Gesetzes der Multiplikation die Gesetze gelten:

---

[4]) Man vgl. hierzu: W. Magnus: a) Über Beziehungen zwischen Gruppen und Idealen in einem speziellen Ring. Mathematische Annalen **111**, 259—280, 1935. b) Journal für die reine und angewandte Mathematik **177**, 105—115, 1937. c) Monatshefte für Mathematik und Physik **47**, 307—313, 1939.

[5]) E. Witt, Journal für die reine und angewandte Mathematik **177**, 152—160, 1937.

$$[\varphi\psi] + [\psi\varphi] = 0 \tag{5}$$
$$\varphi[\psi\chi] + \psi[\chi\varphi] + \chi[\varphi\psi] = 0.$$

Man betrachte nun einen freien Lieschen Ring Λ mit Erzeugenden $\xi, \eta, \ldots$, wobei das Wort „frei" bedeuten soll, daß zwischen $\xi, \eta, \ldots$ und ihren Produkten nur solche Beziehungen bestehen sollen, die allein aus den Rechengesetzen folgen. Man erhält dann eine treue Darstellung von Λ in $\mathfrak{R}$, wenn man folgende Zuordnungen trifft [4b,5]):

$$\xi \to x,\ \eta \to y, \ldots; \text{ Summe in } \Lambda \to \text{Summe in } \mathfrak{R}. \tag{6}$$
$$\text{Mit } \varphi \to f(x, y, \ldots),\ \psi \to g(x, y, \ldots) \text{ gelte } [\varphi\psi] \to fg - gf.$$

Dabei gilt dann, daß die möglichen Polynome $D(W) = d_n$ gerade alle und nur die Elemente von $\mathfrak{R}$ sind, welche bei der Zuordnung (6) als Bilder eines homogenen Polynoms n-ten Grades in $\xi, \eta, \ldots$ mit ganzzahligen Koeffizienten in $\mathfrak{R}$ auftreten. Es gibt also genau ein Polynom $\delta_n(\xi, \eta, \ldots)$ vom n-ten Grade in Λ, so daß

$$\delta_n(\xi, \eta, \ldots) \to d_n(x, y, \ldots).$$

Wir setzen $\delta_n \equiv \Delta(W)$, und bezeichnen d_n auch als *Wert von* δ_n *in* $\mathfrak{R}$; in diesem Sinne schreiben wir kurz

$$d_n = \overline{\delta_n(\xi, \eta, \ldots)}, \text{ also } x = \bar{\xi},\ xy - yx = \overline{[\xi\eta]}, \text{ usw.} \tag{7}$$

Schließlich treffe man noch folgende Festsetzungen: Man betrachte alle Elemente aus $\mathfrak{F}_n$, die nicht in $\mathfrak{F}_{n+1}$ liegen. Ihnen sind zugeordnet gewisse Polynome n-ten Grades d_n aus $\mathfrak{R}$. Wir notieren uns alle diejenigen d_n, die gleich einem $D(W)$ sind, wobei W in $\{(\mathfrak{R}, \mathfrak{F}_n), \mathfrak{F}_{n+1}\}$ liegt. Sie bilden, bei Hinzufügung der Null, einen Modul $\mathfrak{M}_n$ von homogenen Polynomen n-ten Grades aus $\mathfrak{R}$; den Modul aller d_n nennen wir P_n. Dann gilt:

$$\mathfrak{A}_n \simeq P_n/\mathfrak{M}_n, \tag{8}$$

beide Moduln als additive Abelsche Gruppen aufgefaßt. Es ist weiterhin sowohl $\mathfrak{M}_n$ wie P_n Bild eines Moduls aus homogenen Polynomen n-ten Grades M_n bzw. Λ_n aus Λ; Λ_n ist der Modul aller homogenen Polynome n-ten Grades in $\xi, \eta, \ldots$ mit ganzzahligen Koeffizienten. Jetzt erhält man den Satz:

I. *Die Summe aller Moduln* M_n *bildet ein Ideal* M *in* Λ. *Der Liesche Quotientenring* $\Lambda/\mathsf{M} = \Lambda^*$ *ist unabhängig von der Wahl der Erzeugenden eindeutig durch* $\mathfrak{G}$ *bestimmt; er heiße der der Gruppe* $\mathfrak{G}$ *zugeordnete Liesche Ring.* Λ^* *ist nilpotent, und zwar ist* $\Lambda^{*k} = 0$, *wenn* $\mathfrak{G}_k = \mathfrak{G}_{k+1}$ *ist. Wenn* $\mathfrak{G}$ *eine p-Gruppe ist, so enthalten* $\mathfrak{G}$ *und* Λ^* *gleichviele Elemente.*

Daß die Moduln M_n ein Ideal bilden, besagt nur, daß für einen Normalteiler $\mathfrak{N}$ von $\mathfrak{F}$ das Produkt zweier Elemente aus $\mathfrak{N}$ und der Kommutator eines Elementes aus $\mathfrak{N}$ und eines Elementes aus $\mathfrak{F}$ wieder in $\mathfrak{N}$ liegen; aus dieser Bemerkung ergeben sich dann auch die übrigen Behauptungen des Satzes.

5. Es fehlt jetzt noch eine Verbindung zwischen Λ und $\mathfrak{R}$, welche klarstellt, daß in der Tat für die Untersuchung von $\mathfrak{G}$ durch die Zuordnung (2) nur solche Elemente von $\mathfrak{R}$ gebraucht werden, welche Bilder von Elementen aus Λ bei der Zuordnung (6) sind. Zunächst treten ja z. B. in den Ausdrücken für $ab = 1 + x + y + xy$ oder für $aba^{-1}b^{-1}$ in den Gliedern höheren Grades auch Summanden auf, die sich nicht aus Bildern von Elementen aus Λ zusammensetzen lassen (z. B. xy). Der fehlende Zusammenhang wird geleistet durch die sogenannte Hausdorffsche Formel [6]), die man folgendermaßen einführen kann: Es sei $\mathfrak{R}'$ ein weiterer freier Ring von derselben Art wie $\mathfrak{R}$ und mit Erzeugenden $x', y', \ldots$; es sei ferner Λ' ein weiterer Liescher Ring derselben Art wie Λ

[6]) F. Hausdorff, Sitzungsberichte der Sächsischen Akademie der Wissenschaften in Leipzig, Mathematisch-physikalische Klasse, **58**, 19—48, 1906.

mit Erzeugenden $\xi', \eta', \ldots$, nur daß wir jetzt als Elemente von Λ' beliebige Potenzreihen (analog wie bei $\Re$) mit rationalen Koeffizienten zulassen wollen. Nun ordne man zu:

$$\xi' \to x', \quad [\xi'\eta'] \to x'y' - y'x' \text{ usw. wie in (6).} \tag{9}$$

Ferner setze man (das Gleichheitszeichen für die Zuordnung ist hier erlaubt, da sich bei der Zuordnung isomorphe Abbildungen ergeben, wie leicht zu sehen):

$$a = 1 + x = e^{x'} \equiv \sum_{\nu=0}^{\infty} \frac{x'^{\nu}}{\nu!}, \quad b = e^{y'} \equiv \sum_{\nu=0}^{\infty} \frac{y'^{\nu}}{\nu!}, \ldots; \quad x' = \sum_{\nu=1}^{\infty} \frac{(-x)^{\nu+1}}{\nu}, \ldots \text{ usw.} \tag{9'}$$

Dann wird, wie Hausdorff gezeigt hat:

$$ab = e^{x'+y'+\frac{x'y'-y'x'}{2}+\cdots} = e^{\overline{\mathsf{H}(\xi',\eta')}}, \quad \mathsf{H} \equiv \xi' + \eta' + \frac{[\xi'\eta']}{2} + \cdots, \tag{10}$$

und allgemein

$$W(a, b, \ldots) = e^{\overline{\Omega(\xi',\eta',\ldots)}}, \tag{11}$$

wobei Ω ein Element aus Λ' ist, und $\overline{\Omega}$ als „Wert von Ω in $\Re'$“ genau so erklärt ist wie oben der Wert eines Elementes aus Λ in $\Re$ auf Grund von (6) erklärt wurde. Die Potenzreihen Ω besitzen rationale Koeffizienten von nicht bekannter Zusammensetzung; man weiß nur, daß in den Nennern der Koeffizienten von Gliedern eines Grades $< p$ die Primzahl p nicht auftreten kann, und daß andererseits in den Nennern beliebig hohe Potenzen beliebiger Primzahlen als Faktoren enthalten sein können. Die Frage nach den Nennern in den Koeffizienten der Hausdorffschen Formel (10) hängt zusammen mit einer von Hall [2]) entdeckten Identität, die sich übrigens mit den hier entwickelten Hilfsmitteln leicht beweisen läßt[4b]). Im einfachsten Falle lautet die Hallsche Identität: Ist $\mathfrak{F}$ die freie Gruppe mit den freien Erzeugenden $a, b, \ldots$, so ist für jede Primzahl p:

$$(ab)^p \equiv a^p b^p C^p \cdot C_p, \tag{12}$$

wobei C ein Element aus der Kommutatorengruppe $\mathfrak{F}_2$ von $\mathfrak{F}$ und C_p ein Element aus $\mathfrak{F}_p$ ist. Hierbei ist C_p (unabhängig von der möglichen Wahl von C) eindeutig modulo $\mathfrak{F}_{p+1}$ und modulo p-ten Potenzen von Elementen aus $\mathfrak{F}_p$ bestimmt; dies bedeutet, daß $D(C_p)$ eindeutig modulo p bestimmt ist. Ist nun $\mathsf{H}_p(\xi', \eta')$ der homogene Bestandteil p-ten Grades von H aus (10), so gilt

$$p\,\overline{\mathsf{H}_p(\xi', \eta')} \equiv D(C_p) \text{ mod. } p. \tag{13}$$

$D(C_p)$ berechnet sich also eindeutig aus den Gliedern von H_p, deren Nenner den Faktor p enthalten. Die explizite Kenntnis von C_p ist für manche Zwecke sehr interessant, sie spielt insbesondere für ein Problem von Burnside [7]) eine wichtige Rolle; man kennt indessen die Koeffizienten der Hausdorffschen Formel so wenig, daß man zur Berechnung von $D(C_p)$ auf andere, von O. Grün [8]) und H. Zassenhaus [9]) entdeckte Methoden zurückgreifen muß.

6. Um die durch Satz I erklärte Zuordnung eines Lieschen Ringes Λ^* zu einer Gruppe $\mathfrak{G}$ nutzbar zu machen, ist zunächst die Frage zu untersuchen, inwieweit umgekehrt zu jedem Lieschen Ring mit den ganzen Zahlen als Koeffizientenbereich eine Gruppe gehört, der dieser Liesche Ring zugeordnet ist, vorausgesetzt, daß dieser Liesche Ring „homogene“ Relationen besitzt, d. h. daß er sich aus einem freien Lieschen Ring

---

[7]) W. Burnside, Quarterly Journal of Mathematics **33**, 230—238, 1902. Vgl. die Angaben in der unter [8]) zitierten Arbeit von O. Grün.

[8]) O. Grün, in diesem Bande. Ebenda auch weitere Identitäten vom Charakter der Hallschen Identität (12) und nähere Angaben über die Bedeutung der Berechnung von C_p.

[9]) H. Zassenhaus, Abhandlungen aus dem Mathematischen Seminar der Hansischen Universität Hamburg **13**, 1—100, besonders 90—95, 1939.

durch Hinzufügen von Relationen definieren läßt, die in den Erzeugenden des Ringes homogen sind. (Als solche Relationen kann man wählen: Erzeugende Elemente der Moduln M_n gleich Null.) Der wichtigste Spezialfall dieser Frage ist der, daß der gegebene Liesche Ring Λ^* nilpotent ist, und daß seine Elemente mit einer Potenz der Primzahl p multipliziert gleich Null werden; Λ^* muß dann einer p-Gruppe $\mathfrak{P}$ zugeordnet sein, wenn es überhaupt eine Gruppe gibt, der Λ^* zugeordnet ist. Es sei also

$$\Lambda^{*k} = 0; \quad p^m \Lambda^* = 0. \tag{14}$$

Dann gilt der Satz:

II. *Wenn $k \leqq p$ ist und die Beziehungen* (14) *erfüllt sind, so gibt es mindestens eine Gruppe $\mathfrak{P}$, deren Ordnung eine Potenz von p ist, so daß Λ^* der nach Satz* I *der Gruppe $\mathfrak{P}$ zugeordnete Liesche Ring ist.*

Der Beweis läßt sich ohne Mühe mit Hilfe der Hausdorffschen Formel (11) erbringen, indem man einfach für $\xi', \eta', \ldots$ Erzeugende von Λ^* einsetzt, und durch (9), (9'), (2) eine Gruppe mit den Erzeugenden $a, b, \ldots$ konstruiert. Da wegen $k \leqq p$ hier der Nenner p in der Hausdorffschen Formel nicht auftritt, sind dann nämlich alle in (11) auftretenden Funktionen $\Omega(\xi', \eta', \ldots)$ wieder Elemente von Λ^*. Man kann dann weiter mit geringer Mühe zeigen, daß der dieser Gruppe zugeordnete Liesche Ring wirklich wieder isomorph mit Λ^* ist. Die Voraussetzung $k \leqq p$ kann in Satz II nicht entbehrt werden, es gilt nämlich als Ergänzung zu II:

IIa. *Es gibt keine Gruppe $\mathfrak{P}$, deren nach Satz I zugeordneter Liescher Ring der Ring Λ^* von zwei Erzeugenden ξ, η mit $\Lambda^{*p+2} = p\Lambda^* = 0$ ist, wobei in Λ^* keine Relationen bestehen sollen, die nicht aus diesen Forderungen folgen.*

Wäre nämlich $\mathfrak{P}$ eine Gruppe, der der Liesche Ring Λ^* aus IIa zugeordnet ist, so müßte es auch eine p-Gruppe geben, der Λ^* zugeordnet ist. Diese heiße wieder $\mathfrak{P}$. Es besäße dann $\mathfrak{P}$ zwei Erzeugende a, b, es wäre $\mathfrak{P}_{p+2} = 1$ und es würde (für $k = 1, \ldots, p+1$) die p-te Potenz jedes Elementes aus $\mathfrak{P}_k$ in $\mathfrak{P}_{k+1}$ liegen. Andererseits wäre für ein beliebiges Wort $W(a, b)$ aus a und b stets $W(a, b)$ ein Element aus $\mathfrak{P}_k$ aber nicht aus $\mathfrak{P}_{k+1}$, wenn $D(W)$ vom k-ten Grade und inkongruent Null modulo p ist. Nun folgt aus der Hallschen Identität, daß ab mit $a^p b^p C^p C_p$ vertauschbar ist; $a^p b^p C^p C_p$ ist nach dem oben Bemerkten ein Element Γ aus $\mathfrak{P}_2$; liegt nun Γ nicht in $\mathfrak{P}_{p+1}$, sondern in einer Untergruppe $\mathfrak{P}_k$ mit $2 \leqq k \leqq p$, so ist Γ gleich einem Wort $W(a, b)$, so daß $D(W)$ den Grad k hat und $\not\equiv 0 \bmod p$ ist. Dann besitzt aber $D(ab\Gamma b^{-1}a^{-1}\Gamma^{-1})$ den Grad $k+1$ und ist ebenfalls $\not\equiv 0 \bmod p$, wie man leicht nachrechnet, und wie übrigens auch aus einem an anderer Stelle[4b]) bewiesenen Satz folgt. Da andererseits $ab\Gamma b^{-1}a^{-1}\Gamma^{-1}$ gleich 1 sein muß, folgt also, daß Γ in $\mathfrak{P}_{p+1}$ liegen muß. Dann müssen aber, wie man leicht sieht, die p-ten Potenzen aller Elemente von $\mathfrak{P}$ in $\mathfrak{P}_{p+1}$ liegen; es wäre also $\mathfrak{P}/\mathfrak{P}_{p+1} = \mathfrak{G}$ eine p-Gruppe, in der jede p-te Potenz gleich 1 wäre, und der $\mathfrak{G}$ zugeordnete Liesche Ring Λ' wäre genau so beschaffen wie Λ^*, nur daß jetzt $\Lambda'^{p+1} = 0$ wäre. Andererseits wäre dann in $\mathfrak{G}$ sicher $C_p = 1$, entgegen der von Grün[8]) und Zassenhaus[9]) bewiesenen Tatsache, daß $D(C_p)$ vom Grade p ist und $\not\equiv 0 \bmod p$ ist. Bei der Beschaffenheit von Λ' dürfte also C_p nicht $= 1$ sein, und damit ist gezeigt, daß $\mathfrak{G}$ und mithin auch $\mathfrak{P}$ nicht existieren kann.

Aus IIa folgt, daß, mindestens für p-Gruppen, die durch Satz I vorgenommene Zuordnung eines Lieschen Ringes zu einer Gruppe nicht die günstigste ist. In der Tat scheint es so zu sein, daß bei der von H. Zassenhaus[10]) mitgeteilten Zuordnung eines Lieschen Ringes mit der Charakteristik p zu einer p-Gruppe nicht der Fall eintreten

---

[10]) H. Zassenhaus, Abhandlungen aus dem Mathematischen Seminar der Hansischen Universität Hamburg **13**, 200–207, 1940.

kann, daß zu einem Lieschen Ring der von Zassenhaus angegebenen Art keine p-Gruppe gehört, der er zugeordnet ist. Ein Beweis hierfür fehlt allerdings vorläufig noch; jedenfalls aber dürfte die von Zassenhaus angegebene Zuordnung eines Lieschen Ringes zu einer p-Gruppe die zweckmäßigere sein.

7. Eine Frage, die mit den Sätzen I und II unmittelbar zusammenhängt, ist die folgende:

Jeder Relation $R(a, b, \ldots) = 1$ zwischen den Erzeugenden der Gruppe $\mathfrak{G}$ entspricht eine Relation, die man in dem Ring $\mathfrak{R}$ mit den Erzeugenden $x, y, \ldots$ oder in dem Lieschen Ring Λ der Erzeugenden $\xi', \eta', \ldots$ ansetzen kann; ist nämlich

$$R(a, b, \ldots) \equiv 1 + F(x, y, \ldots) = e^{\overline{\Omega(\xi', \eta', \ldots)}},$$

so kann man setzen: $F = 0$ bzw. $\Omega(\xi', \eta', \ldots) = 0$. Indem man zu jeder Relation $R = 1$ die zugehörige Relation $\Omega = 0$ bildet, erhält man aus Λ' einen Ring $\overline{\Lambda}$, und wenn man nun $\xi', \eta', \ldots$ als Erzeugende von $\overline{\Lambda}$ betrachtet, liefern die Beziehungen (10), (11) (9′), (9) eine Darstellung der Gruppe $\mathfrak{G}$. Es fragt sich, wann dieselbe treu sein wird. Dies kann natürlich nur der Fall sein, wenn der Durchschnitt aller Gruppen $\mathfrak{G}_k$ das Einheitselement ist; es ist sicher der Fall, wenn $\mathfrak{G}$ eine p-Gruppe mit $\mathfrak{G}_p = 1$ ist, wie unmittelbar aus dem über die Hausdorffsche Formel Gesagten zu entnehmen ist. *Für p-Gruppen mit $\mathfrak{G}_p = 1$ bekommt man auf diese Weise eine umkehrbar-eindeutige Beziehung zwischen diesen und endlichen Lieschen Ringen $\overline{\Lambda}$, für die $\overline{\Lambda}^p = 0$ und $q\overline{\Lambda} = 0$ ist, wobei q eine Potenz von p ist*; die Relationen von $\overline{\Lambda}$ sind dabei i. a. nicht mehr homogen (s. o.). Inwieweit sich eine solche Beziehung für umfassendere Klassen von p-Gruppen herstellen läßt, ist eine noch offene Frage. Man vergleiche hierzu auch H. Zassenhaus [10]).

8. Zum Schluß sei noch auf ein an anderer Stelle[4a]) erwähntes Problem hingewiesen, für welches die Zuordnung eines Lieschen Ringes zu einer Gruppe ebenfalls nutzbar gemacht werden kann. Es wäre nämlich sowohl für die Untersuchung der Automorphismen einer durch Erzeugende und definierende Relationen gegebenen Gruppe als auch für die Frage nach den durch reine Kommutatorbildung erklärbaren vollinvarianten Untergruppen einer freien Gruppe sehr wichtig, zu wissen: Welches sind die im Ring der ganzen Zahlen irreduziblen Darstellungsmoduln innerhalb des Moduls der Polynome $d_n(x, y, \ldots)$ aus (3) (bei festem n) für die Gruppe der linearen Substitutionen mit ganzzahligen Koeffizienten der Variabeln $x, y, \ldots$? Dies ist gleichbedeutend mit der Frage nach den irreduziblen Darstellungsmoduln derselben Substitutionsgruppe, geschrieben mit den Erzeugenden $\xi, \eta, \ldots$ eines freien Lieschen Ringes als Variablen; insbesondere wäre es interessant zu wissen, *ob es im freien Lieschen Ring Λ mit den Erzeugenden $\xi, \eta, \ldots$ Invarianten gegenüber der Gruppe aller umkehrbaren linearen Substitutionen von $\xi, \eta, \ldots$ gibt*; die Voraussetzung, daß die Substitutionskoeffizienten ganz sein sollen, kann offenbar weggelassen werden, da sie keine Einschränkung bedeutet. Man weiß hierüber folgendes:

Es sei k die Anzahl der Erzeugenden $\xi, \eta, \zeta, \ldots$ des Lieschen Ringes Λ. Dann gibt es gegenüber der Gruppe der unimodularen Substitutionen von $\xi, \eta, \zeta, \ldots$ Invarianten, wenn $k = 2$ ist, und zwar gibt es zu jedem Grade m, der das Doppelte einer ungeraden Zahl ist, mindestens eine Invariante, z. B. für $m = 2, 6, \ldots$ die Invarianten

$$[\xi, \eta], \quad [[\xi, [\xi, \eta]], \ [\eta, [\xi, \eta]]] \text{ usw.}$$

Für die Werte von $m > 6$ gibt es im allgemeinen mehrere Invarianten. — Für $k > 2$ läßt sich zeigen, daß es keine Invarianten von einem Grade $< 2k$ gibt. Es kann allgemein nur Invarianten geben, deren Grad ein Vielfaches von k ist. Ferner läßt sich ein Verfahren

angeben, um alle Invarianten zu finden. Jedem homogenen Polynom in $\xi, \eta, \ldots$ entspricht nach (6) eindeutig ein homogenes Polynom in den Variablen $x, y, \ldots$, und diesem läßt sich wiederum ein homogenes Polynom gleichen Grades in kommutativen Variablen zuordnen. Es genügt, eine solche Zuordnung für die Potenzprodukte von $x, y, \ldots$ zu treffen. Es sei m der Grad des betrachteten Potenzproduktes. Jeder der nicht-kommutativen Variablen $x, y, \ldots$ ordne man dann m kommutative Variable zu; es seien etwa $x_1, \ldots x_m$ bzw. $y_1, \ldots, y_m$ usw. zugeordnet zu x bzw. y usw. Dann ordne man jedem Produkt von $x, y, \ldots$ ein solches Produkt der Variablen $x_1, \ldots, x_m$; $y_1, \ldots, y_m$ usw. zu, in dem der Index die Stelle angibt, an der die gleichbezeichnete Variable in dem nicht kommutativen Produkt steht. Es sollen also z. B. die in der folgenden Tabelle untereinanderstehenden Produkte einander zugeordnet sein

$$\begin{array}{cccccc} x & y & x^n & xy^2 & yxxy & \ldots \\ x_1 & y_1 & x_1 \ldots x_n & x_1 y_2 y_3 & y_1 x_2 x_3 y_4 & \ldots . \end{array}$$

Einer Summe sei dann die entsprechende Summe zugeordnet. Es fragt sich nun, wie man diejenigen homogenen Polynome in den Variablen $x_1, \ldots, x_m$; $y_1, \ldots, y_m$; $\ldots$ charakterisieren kann, die solchen homogenen Polynomen m-ten Grades in $x, y, \ldots$ zugeordnet sind, welche ihrerseits Bilder von Polynomen m-ten Grades in dem freien Lieschen Ring sind, der von $\xi, \eta, \ldots$ erzeugt wird. Wir wollen derartige Polynome in den Variablen $x_1, \ldots, x_m$; $y_1, \ldots, y_m$; $\ldots$ „Liesche Formen" nennen, und die Variablen nur durch einen Buchstaben $x_\mu, y_\mu, \ldots$ $(\mu = 1, \ldots, m)$ andeuten. Nun gilt: Ein homogenes Polynom m-ten Grades $P(x_\mu, y_\mu, \ldots)$ ist dann und nur dann eine Liesche Form, wenn es ein weiteres homogenes Polynom $Q(x_\mu, y_\mu, \ldots)$ m-ten Grades gibt, so daß P aus Q durch Anwendung des Operators

$$(1 - \pi_m)(1 - \pi_{m-1}) \cdots (1 - \pi_2) \equiv \omega$$

hervorgeht, wobei ω ein Element des Gruppenringes der symmetrischen Gruppe der Permutationen von m Dingen ist; 1 bedeutet die identische Permutation, π_k bedeutet die Permutation

$$\begin{pmatrix} 1 & 2 & \cdots & k-1 & k & k+1 \cdots m \\ 2 & 3 & \cdots & k & 1 & k+1 \cdots m \end{pmatrix}.$$

Der Operator ω ist auf die Indizes der Variabeln in Q anzuwenden und im übrigen distributiv. Nun läßt sich zeigen: *Ist eine Liesche Form $P(x_\mu, y_\mu, \ldots)$ vom m-ten Grade das Bild einer Invariante m-ten Grades aus den Erzeugenden $\xi, \eta, \ldots$ des freien Lieschen Ringes Λ, so muß es eine simultane Invariante $J(x_\mu, y_\mu, \ldots)$ m-ten Grades der Variablenreihen*

$$x_1, y_1, \ldots; \; x_2, y_2, \ldots; \; \ldots; \; x_m, y_m, \ldots,$$

geben, so daß

$$P(x_\mu, y_\mu, \ldots) \equiv \omega J(x_\mu, y_\mu, \ldots)$$

wird. Zum Beispiel ist für zwei Variable und den Grad 2:

$$x_1 y_2 - x_2 y_1 \equiv (1 - \pi_2)\left(\frac{x_1 y_2 - x_2 y_1}{2}\right).$$

Man kennt nun alle Formen $J(x_\mu, y_\mu, \ldots)$; sie sind Produkte aus Determinanten

$$\begin{vmatrix} x_{\mu_1} & y_{\mu_1} & \cdots \\ x_{\mu_2} & y_{\mu_2} & \cdots \\ \cdot & \cdot & \cdots \\ x_{\mu_k} & y_{\mu_k} & \cdots \end{vmatrix},$$

wobei k die Anzahl der Variablen $\xi, \eta, \ldots$ bedeutet. Die Schwierigkeit besteht dann darin, festzustellen, ob durch Anwendung des Operators ω alle Formen J identisch Null werden; dies ist für $m = k$ der Fall; es ist z. B. für $m = k = 3$

$$(1 - \pi_3)\,(1 - \pi_2) \begin{vmatrix} x_1 & y_1 & z_1 \\ x_2 & y_2 & z_2 \\ x_3 & y_3 & z_3 \end{vmatrix} \equiv 0.$$

Man darf vielleicht erwarten, daß die hier aufgeworfene kombinatorische Frage sich mit Hilfe der „quantitative substitutional analysis“ von A. Young [11]) lösen läßt. Sie läßt sich, ebenso wie einige verwandte Fragen, auf Untersuchungen allein über den Gruppenring der symmetrischen Gruppe zurückführen [12]).

[11]) A. Young, Proceedings of the London Mathematical Society (1), **33**, 97—146, 1901; **34**, 361—397, 1902.

[12]) Man vergleiche § 3 der Arbeit von O. Grün in diesem Bande. Die oben gegebene Beschreibung der „Lieschen Formen“ verdanke ich einer mündlichen Mitteilung von Herrn Grün.

Eingegangen 30. Januar 1940.

Darstellungstheorie nilpotenter Lie-Ringe bei Charakteristik $p > 0$*).

Von *Hans Zassenhaus* in Hamburg.

Herr Magnus hat ein Verfahren beschrieben, wie man jeder p-Gruppe einen Lie-Ring zuordnen kann, dessen Charakteristik eine p-Potenz ist. Gewisse Eigenschaften der p-Gruppen übertragen sich auf die zugeordneten Lie-Ringe, wenn man Aussagen über Multiplikation und Kommutatorbildung in Gruppen Aussagen über Addition und Multiplikation in Lie-Ringen entsprechen läßt. Dieses Prinzip:

Gruppe → Lie-Ring,

Multiplikation → Addition

Kommutatorbildung → (Kreis-, Klammer-)Multiplikation

erweist sich überhaupt als fruchtbar. Es gibt zum Beispiel eine wichtige Identität in Gruppen, die von Hall stammt und von ihm mit großem Erfolg in der Theorie der p-Gruppen angewendet worden ist, nämlich die folgende:

Für jede natürliche Primzahl p ist

$$(1) \qquad (xy)^p = x^p y^p c^p z_p;$$

dabei liegt c in der Kommutatorgruppe der aus x und y erzeugten Gruppe, z_p ist ein Produkt von mehrfachen Kommutatoren, die je p Komponenten aus der von x und y erzeugten Gruppe haben.

Lassen wir nun noch dem Potenzieren mit p das Potenzieren mit p entsprechen, so lautet das Analogon zu der Hallschen Identität in Lie-Ringen folgendermaßen:

$$(2) \qquad (x + y)^p = x^p + y^p + \Lambda(x, y) + p P(x, y),$$

wobei x und y als Elemente eines assoziativen Ringes aufzufassen sind. Dabei ist $\Lambda(x, y)$ ein explizit angebbarer Ausdruck in x und y, der durch Addition mehrerer Liescher Produkte mit je p Faktoren x oder y entsteht. Als Liesches Produkt möge dabei der Ausdruck

$$u \circ v = uv - vu$$

bezeichnet werden; denn nach dieser neuen Multiplikation bildet der ursprünglich vorliegende Ring unter Beibehaltung der alten Addition einen Lie-Ring. $P(x, y)$ ist ein homogenes Polynom p-ten Grades mit ganzen Koeffizienten in x und y.

Der Beweis der Identität (2), die wohl als erster Jacobson veröffentlicht hat, möge hier nach Artin gegeben werden:

*) Vergl. H. Zassenhaus, Über Liesche Ringe mit Primzahlcharakteristik, Abhandl. Math. Seminar Hamburg **13** (1939), 1—100.

Zu dem nichtkommutativen Polynombereich $\mathfrak{P} = k[x_1, x_2, \ldots, x_n]$ über einem Körper k mit der Charakteristik p adjungiere man n untereinander und mit den x_i vertauschbare Variable $t_1, t_2, \ldots, t_n$. In dem neuen Polynombereich in $t_1, t_2, \ldots, t_n$ mögen in der üblichen Weise Differentiale mit $\mathfrak{P}$ als Konstantenbereich definiert werden. Dann berechne man das Differential von

$$(t_1 x_1 + t_2 x_2 + \cdots + t_n x_n)^p$$

auf zwei Weisen. Es gilt für beliebiges z die folgende Potenzregel:

$$dz^m = \sum_{i=1}^{m} \binom{m}{i} ((\underline{z})^{m-1} dz) z^{m-i}, \tag{3}$$

wie man durch vollständige Induktion leicht beweist. Dabei bedeute $\underline{z}$, $\underline{u}$, $\underline{x}$ usw. stets die Lie-Multiplikation mit z, u, x usw. von links her, z. B. $\underline{z}a = za - az$. Man setze $z = t_1 x_1 + t_2 x_2 + \cdots + t_n x_n$ und findet, daß einerseits

$$dz^p = (\underline{z})^{p-1} dz, \tag{4}$$

weil die Binomialkoeffizienten $\binom{p}{i}$ $(0 < i < p)$ in einem Körper mit der Charakteristik p verschwinden. Andererseits wird der Ansatz

$$(\Sigma t_i x_i)^p = \sum_{1}^{n} t_i^p x_i^p + \sum_{\mu}{}' t_1^{\mu_1} t_2^{\mu_2} \cdots t_n^{\mu_n} \Lambda_{p,\mu}(x_1, \ldots, x_n) \tag{5}$$

gemacht, in der die Summe mit dem Akzent über die nicht trivialen Partitionen μ von p in n Summanden erstreckt werden möge. Die rechte Seite der angesetzten Gleichung möge ebenfalls differenziert werden und das Resultat mit der Gleichung (4) verglichen werden. Dann ergeben sich explizite Darstellungen der Polynome $\Lambda_{p,\mu}(x)$ als Summen über gewisse Kreisprodukte mit je p Faktoren x_1 oder x_2 ... oder x_n.

Durch mehrfache Anwendung der vorstehenden Formel wird die folgende Formel für die p^ϱ-te Potenz einer endlichen Summe erhalten:

$$\begin{aligned}(t_1 x_1 + t_2 x_2 + \cdots + t_n x_n)^{p^\varrho} &= t_1^{p^\varrho} x_1^{p^\varrho} + \cdots + t_n^{p^\varrho} x_n^{p^\varrho} + \cdots \\ &= \sum_{\nu=0}^{\varrho} \sum_{\mu} t_1^{\mu_1} \cdots t_n^{\mu_n} \Lambda_{p^\nu,\mu}^{p^{\varrho-\nu}}(x_1, \ldots, x_n),\end{aligned} \tag{6}$$

in der die innere Summe jeweils über alle Partitionen von p^ν in n Summanden erstreckt wird und die $\Lambda_{p^\nu,\mu}(x)$ rekursiv und unabhängig von ϱ definierte Summen aus Lie-Produkten mit je p^ν Faktoren x_1 oder x_2 ... oder x_n sind.

Mit Hilfe dieser direkten Ableitung und Zuhilfenahme der Magnusschen Dimensionstheorie läßt sich ein kurzer Beweis der Hallschen Formel angeben, ferner kann man eine Fülle von anderen gruppentheoretischen Identitäten herleiten, worüber Herr Grün vortragen wird.

Ich will Ihnen hier von einer Anwendung berichten, die sich auf die Darstellungstheorie der nilpotenten Lie-Ringe mit Primzahlcharakteristik machen läßt. Dabei wird die Formel kombiniert mit der bekannten Formel von Cartan-Weyl:

$$x^n y = \sum_{0}^{n} \binom{n}{i} ((\underline{x})^i y) x^{n-i}, \tag{7}$$

die man durch vollständige Induktion leicht als richtig erkennt. Wenn in der letzten Formel für n eine p-Potenz eingesetzt wird, so verschwinden bei Charakteristik p alle Binomialkoeffizienten, die nicht am Anfang oder Ende stehen, und es bleibt eine Formel von der Gestalt

$$x^{p^\nu} y - y x^{p^\nu} = (\underline{x})^{p^\nu} y \tag{8}$$

übrig; d. h. in assoziativen Ringen von der Charakteristik p ist Lie-Multiplikation mit der p^ν-ten Potenz eines Basiselementes dasselbe wie p^ν-malige Lie-Multiplikation mit der Basis.

Es sei H ein endlicher nilpotenter Lie-Ring über algebraisch abgeschlossenem Grundkörper k mit der Charakteristik $p > 0$. Es gibt also eine Zahl c, so daß jedes mehrfache Lie-Produkt aus $c + 1$ Faktoren verschwindet. Gesucht werden die irreduziblen Darstellungen endlichen Grades von H.

Es sei Δ eine irreduzible Darstellung vom Grade f, $\mathfrak{M}$ sei ein zu Δ gehöriger Darstellungsmodul, so daß dem Element h aus H die lineare Transformation Δh von $\mathfrak{M}$ zugeordnet wird. Δh hat wenigstens einen Eigenwert αh, und die zu diesem Eigenwert gehörigen Eigenvektoren, das sind alle Elemente u aus $\mathfrak{M}$, für die

$$(\Delta h - \alpha h)^\nu u = 0 \quad \text{für alle großen } \nu,$$

bilden einen Teilmodul $\mathfrak{M}'$. Aber $\mathfrak{M}'$ ist unter H invariant. Denn: Es sei u ein Vektor aus $\mathfrak{M}'$, so daß die obenstehende Gleichung erfüllt ist. Dann setze man in der Formel (7) ein:

$$x = \Delta h - \alpha h,$$
$$y = \Delta h' \text{ beliebig aus } \Delta H,$$
$$n = \nu + c,$$

und wende beide Seiten auf den Vektor u an. Rechts verschwindet zufolge der Voraussetzungen aber jeder Summand. Es folgt, daß

$$(\Delta h - \alpha h)^n h' u = 0,$$

d. h. auch $h'u$ gehört zu $\mathfrak{M}'$, also ist $\mathfrak{M}'$ unter H invariant. Da aber Δ irreduzibel und $\mathfrak{M}'$ von 0 verschieden ist, so ist $\mathfrak{M}' = \mathfrak{M}$, d. h. durch eine irreduzible Darstellung wird jedem Element h aus H genau *ein* Eigenwert αh zugeordnet. Welche Eigenschaften haben nun diese auf H eindeutig definierten Eigenfunktionen?

Um das zu beantworten, wird eine Basis $a_1, a_2, \ldots, a_r$ von H gewählt und der Eigenwert von $h = \lambda_1 a_1 + \lambda_2 a_2 + \cdots + \lambda_r a_r$ als Funktion der λ_i ausgedrückt. Man suche nämlich eine p-Potenz p^ϱ, die mindestens so groß wie c ist, und wende die Formel (6) an. Man erhält:

$$(\Delta h)^{p^\varrho} = \Big(\sum_{i=1}^{r} \lambda_i \Delta a_i\Big)^{p^\varrho} = \sum_{i=1}^{r} (\lambda_i \Delta a_i)^{p^\varrho} + \sum_{\mu}{}' \ldots + \cdots.$$

Wird nun für die p^ϱ-te Potenz links oder für einen Summanden rechts das Lie-Produkt mit einem beliebigen $\Delta h'$ aus Δh gebildet, so läßt sich dieses Lie-Produkt stets in ein solches mit je $p^\varrho + 1$ Faktoren aus ΔH verwandeln, und da $p^\varrho + 1 \geqq c + 1$, so wird stets Null entstehen. Nach dem Lemma von Schur sind aber Matrizen, die mit allen Matrizen einer irreduziblen Darstellung elementweise vertauschbar sind, skalare Vielfache der Einheitsmatrix, so daß in der Formel an die Stelle der Matrizen ihre Eigenwerte gesetzt werden dürfen. Dann entsteht aber eine Formel von der Gestalt

$$(\alpha h)^{p^\varrho} = \Psi(\lambda_1, \ldots, \lambda_r;\ \alpha_1, \ldots, \alpha_r;\ \beta_{p^\nu, \mu}^{p^\varrho - \nu}),$$

in der $\alpha_i = \alpha a_i$ gesetzt ist, $\beta_{p^\nu, \mu}$ der Eigenwert von $\Lambda_{p^\nu, \mu}(a_1, a_2, \ldots, a_r)$ ist und ν von 1 bis ϱ läuft. Das Polynom Ψ ist bei festem α, β homogen vom Grade p^ϱ in den λ und hat als Polynom der α, β allein betrachtet kein konstantes Glied.

Die Formel wird noch einfacher, wenn die Basis $a_1, a_2, \ldots, a_r$ *regulär* ist, d. h., die Elemente $a_1, a_2, \ldots, a_i$ sollen jeweils die Basis eines Teilringes H_i sein, so daß $0 = H_0 < H_1 < \cdots < H_r = H$ gilt. Ein nilpotenter Lie-Ring hat stets eine reguläre Basis, und es werde von nun ab stets vorausgesetzt, daß *die Basis* $a_1, a_2, \ldots, a_r$ *regulär*

ist. Ähnlich wie in p-Gruppen gezeigt wird, daß eine maximale Untergruppe stets Normalteiler ist, so wird für nilpotente Lie-Ringe gezeigt, daß maximale Teilringe stets Ideale sind. In unserem Falle folgt, daß H_i Ideal von H_{i+1} ist. Beispielsweise liegt das Lie-Produkt eines Elementes aus H mit einem Element aus H_{r-1} in H_{r-1}. Jetzt kann durch Induktion nach r leicht geschlossen werden, daß sich die $\beta_{p^\nu,\mu}$ als Polynome ohne konstantes Glied in den α_i ausdrücken lassen und folglich für den Eigenwert die Formel

$$(9) \qquad (\alpha h)^{p^\varrho} = \Phi(\lambda_1, \lambda_2, \ldots, \lambda_r;\ \alpha_1, \alpha_2, \ldots, \alpha_r)$$

erhalten wird, in der das Polynom Φ bei festen α in den λ homogen vom Grade p^ϱ ist und kein in den α konstantes Glied vorkommt.

Der Eigenwert eines beliebigen Elementes ist also durch die Eigenwerte der Elemente einer regulären Basis eindeutig bestimmt. Es fragt sich nun, ob man diese Eigenwerte willkürlich vorschreiben darf. Das wird bejahend beantwortet werden durch die Konstruktion einer Darstellung mit vorgegebenem eindeutigen Eigenwert α_i für das Basiselement a_i $(i = 1, 2, \ldots, r)$. Die irreduziblen Komponenten dieser Darstellung werden dann ebenfalls eindeutig die vorgeschriebenen Eigenwerte in den Basiselementen annehmen.

Für 1-gliedrige Lie-Ringe $H = \{a_1\}$ liefert offenbar die irreduzible Darstellung $\lambda a_1 \to \{\lambda\alpha_1\}$ jede mögliche Eigenwertverteilung. Nun sei $r > 1$ und es werde die Induktionsvoraussetzung gemacht, daß sich für $(r-1)$-gliedrige Lie-Ringe zu vorgegebenen Eigenwerten der Elemente einer regulären Basis stets eine Darstellung konstruieren läßt. $a_1, a_2, \ldots, a_{r-1}$ ist eine reguläre Basis von H_{r-1}, also gibt es eine Darstellung Γ von H_{r-1}, bei der a_i nur den einen Eigenwert α_i besitzt. Dann lautet die Vorschrift zur Konstruktion der gesuchten Darstellung von H wie folgt:

Dem Element a_r ist die lineare Transformation $\underline{a}_r = \begin{pmatrix} x \\ a_r \circ x \end{pmatrix}$ von H zugeordnet. Unter den linearen Transformationen $\underline{a}_r, \underline{a}_r^p, \ldots, \underline{a}_r^{p^\nu}, \ldots$ gibt es die erste, die von den vorhergehenden linear abhängt, etwa

$$\underline{a}_r^{p^\nu} = \sum_{i=0}^{\nu-1} \lambda_{p^i} \underline{a}_r^{p^i}.$$

Nun ordne man den Basiselementen a_i die folgenden Matrizen zu:

$$a_i \to \left(\binom{\sigma-1}{\tau-1} \Gamma(\underline{a}_r^{\sigma-\tau} a_i)\right) = \begin{pmatrix} \Gamma a_i & 0 & \cdots & 0 \\ \Gamma(\underline{a}_r a_i), & \Gamma a_i & 0 \cdots & 0 \\ \binom{2}{0}\Gamma(\underline{a}_r^2 a_i) & \binom{2}{1}\Gamma \underline{a}_r a_i & \ddots & \vdots \\ \cdots & \cdots & \cdots & \cdots \\ & & & 0 \\ \binom{p^\nu - 1}{0}\Gamma(\underline{a}_r^{p^\nu-1} a_i) & \cdots\cdots & & \Gamma a_i \end{pmatrix},$$

$$a_r \to \begin{pmatrix} 0 & E & & & 0 \\ & 0 & E & & 0 \\ & & \ddots & \ddots & \\ & 0 & & \ddots & \\ & & & & E \\ \alpha_r^{p^\nu} E & \lambda_1 E \cdots & \lambda_p E \cdots & \lambda_{p^{\nu-1}} E \cdots & 0 \end{pmatrix}.$$

Hiernach bleibt nur übrig, die Darstellungsbedingungen zu verifizieren.

Man kommt auf diese Formeln zwangsläufig auf modultheoretischem Wege, indem man sich überlegt, in welcher Weise sich ein irreduzibler Darstellungsmodul von H_{r-1} in einen irreduziblen Darstellungsmodul von H einbetten läßt. Nach Ausführung dieser tiefergehenden Untersuchung kann man auch leicht die irreduzible Darstellung zu gegebener Eigenwertverteilung konstruieren.

Schließlich fragen wir, ob die irreduzible Darstellung durch ihre Eigenfunktion eindeutig bestimmt ist. Hier will ich nicht auf den Mechanismus der Konstruktion näher eingehen, sondern ich werde mich für den Nachweis der Eindeutigkeit einer Schlußweise bedienen, die von Whitehead eingeführt ist und von Witt weitergeführt wurde.

Zu zwei Darstellungen D_1 und D_2 vom Grade f_1 bzw. f_2 von H wird die Produktdarstellung $D = D_1 \times D_2$ folgendermaßen erklärt:

Jedem Element h aus H ordne man eine lineare Transformation Dh des $f_1 \cdot f_2$-dimensionalen Moduls aller rechteckigen Matrizen Λ mit f_1 Zeilen und f_2 Spalten durch die Festsetzung

$$Dh(\Lambda) = D_1 h \cdot \Lambda + \Lambda \cdot (D_2 h)' \tag{10}$$

zu, wobei der Strich den Übergang zur transponierten Matrix angeben soll. Die Darstellungsbedingungen rechnet man leicht als erfüllt nach.

Wenn die Darstellung Γ die eindeutige Eigenfunktion α und Δ die eindeutige Eigenfunktion β besitzt, so besitzt die Produktdarstellung die eindeutige Eigenfunktion $\alpha + \beta$. Wenn nämlich

$$(\Gamma h - \alpha h)^{\nu} = 0, \qquad (\Delta h - \beta h)^{\nu} = 0,$$

so ist

$$(\Gamma \times \Delta(h) - (\alpha + \beta) h)(\Lambda) = (\Gamma h - \alpha h) \cdot \Lambda + \Lambda \cdot (\Delta h - \beta h)',$$

also

$$\begin{aligned}(\Gamma \times \Delta(h) - (\alpha + \beta) h)^{2\nu-1}(\Lambda) &= \sum_{\mu=0}^{2\nu-1} \binom{2\nu - 1}{\mu} (\Gamma h - \alpha h)^{\mu} \cdot \Lambda \cdot (\Delta h - \beta h)^{2\nu-\mu-1} \\ &= 0.\end{aligned}$$

Ferner definiert die Zuordnung $h \to -\Delta' h$ ebenfalls eine Darstellung von H. Diese Darstellung hat die eindeutige Eigenfunktion $-\beta$. Wenn nun $\alpha = \beta$ ist, so hat $\Gamma \times -\Delta'$ nur den Eigenwert 0. Eine Darstellung mit dieser Eigenschaft habe ich *Nildarstellung* genannt. Die irreduziblen Komponenten von Nildarstellungen sind Nulldarstellungen, eine Tatsache, die zum Beweis des Satzes von Engel für Grundkörper beliebiger Charakteristik benutzt wird. In dem vorliegenden Falle folgt, daß es eine von Null verschiedene rechteckige Matrix Λ geben muß, so daß

$$\Gamma \times -\Delta'(\Lambda) \equiv 0.$$

Umgerechnet findet man, daß

$$\Gamma h \cdot \Lambda = \Lambda \cdot \Delta h$$

für alle h aus H gilt. Betrachten wir nun den Fall, daß Γ und Δ zwei irreduzible Darstellungen mit gleicher Eigenfunktion sind, so folgt nach dem Schurschen Verkettungssatz, daß die vorstehenden Gleichungen dann und nur dann in nicht trivialer Weise erfüllt werden können, wenn die beiden Darstellungen äquivalent sind. Damit ist die Eindeutigkeit gezeigt.

Der Grad jeder irreduziblen Darstellung ist eine Potenz von p, evtl. 1. Um das einzusehen, kehren wir noch einmal zu der vorhin ausgeführten Konstruktion zurück. Dabei wurde mittels einer irreduziblen Darstellung Γ von H_{r-1} eine Darstellung Δ von H mit vorgegebener eindeutiger Eigenfunktion α konstruiert, deren Grad aus dem Grad von Γ durch Multiplikation mit einer p-Potenz entstand. Nach dem eben gefundenen Eindeutigkeitssatz folgt, daß Δ nur die eindeutig bestimmte irreduzible Darstellung mit der Eigenfunktion α als Komponente besitzt, so daß der Grad dieser irreduziblen Darstellung ein Teiler des mit einer p-Potenz multiplizierten Grades von Δ ist. Da die Konstruktion bei Darstellungen ersten Grades begann, so folgt durch einen Induktionsschluß, daß der Grad jeder irreduziblen Darstellung von H eine p-Potenz ist.

Eingegangen am 28. Juni 1939.

Verbal and marginal subgroups*).

By *P. Hall* in Cambridge (England).

---

1. Let $f(x_1, \ldots, x_n)$ be any word, i. e. any power-product of the x's and their inverses; and let G be any group. We obtain the *values of f in G* by substituting for the x's in f arbitrary elements of G. These values generate a subgroup of G which will be denoted by $V_f = V_f(G)$. These subgroups, which may be called *verbal subgroups*, are always fully invariant, as has been pointed out by F. Levi.

If $g(y_1, \ldots, y_m)$ is any other word, having no letter in common with f, then we have the commutation rule for verbal subgroups:

$$[V_f, V_g] = V_{[f,g]}.$$

In particular, if we define the commutator words h_i by the rules:

$$h_1 = x_1, \quad h_{i+1} = [h_i, x_{i+1}],$$

then the verbal subgroups

$$V_{h_i} = H_i$$

form the lower central series of G.

Dually, the element ξ may be called a (multiplicative) *period of f in G* if

$$f(x_1, x_2, \ldots, x_n)$$
$$= f(x_1\xi, x_2, \ldots, x_n) = f(x_1, x_2\xi, x_3, \ldots, x_n) = \cdots = f(x_1, x_2, \ldots, x_{n-1}, x_n\xi)$$

for all choices of the x's in G. These periods form a characteristic subgroup $M_f = M_f(G)$, which may be called the *marginal subgroup* (or margin) of G arising from the word f.

If the words f and g have no letters in common, we have the commutation rule for marginal subgroups:

$$M_{[f,g]} = M_f(G \bmod V_g^*) \wedge M_g(G \bmod V_f^*).$$

Here a star denotes a centralizer. And, for instance, $M_f(G \bmod V_g^*)$ is a subgroup M of G which contains the centralizer V_g^* of V_g in G, and which is defined by the rule that $M/V_g^* = M_f(G/V_g^*)$. In particular, we have

$$M_{h_i} = Z_{i-1},$$

the $(i-1)$-th term of the upper central series of G.

Verbal subgroup and marginal subgroup are related by the following

Permutability theorem: If $[\xi, G]$ is contained in $M_f(G)$, then ξ is contained in V_f^*. In other words, V_f^* contains $Z_1(G \bmod M_f)$.

It follows that

$$[V_f, M_f] = 1,$$

---

*) For the results mentioned below, cf. the earlier treatment in Proc. London Math. Soc. (2) **36** (1933), 29—95, especially §§ 2 and 4.

though this is a less precise statement. From the permutability theorem, we have, in particular, that

$$[H_i, Z_i] = 1.$$

A corollary of this is that

$$[H_i, H_j] \leqq H_{i+j},$$

and that if Θ_i is the i-th term of the derived series,

$$\Theta_i \leqq H_{2^i}.$$

2. If G is of order a power of the prime p, it is interesting to consider the words x^{p^k}, involving the single letter x. The corresponding verbal and marginal subgroups may be denoted by $\mathfrak{V}_k$ and Ω_k, respectively. Thus $[\mathfrak{V}_k, \Omega_k] = 1$. We may also consider the characteristic subgroup $\overline{\Omega}_k$ generated by all solutions of the Frobenius equation

$$x^{p^k} = 1.$$

In general these solutions do not constitute a group, so that $\overline{\Omega}_k$ will as a rule contain elements of order greater than p^k; whereas, obviously, every element of Ω_k must satisfy the Frobenius equation. Thus, in general, $\Omega_k < \overline{\Omega}_k$.

There exists, however, an extensive class of p-groups for which $\Omega_k = \overline{\Omega}_k$, for all k. In particular, this is true for *regular* p-groups. It is also true for the class of all subgroups of direct products of regular p-groups, and this class includes certain irregular groups, as is shown by an example[1]) constructed by H. Wielandt. At present, it is known that every p-group of order at most p^p is regular, and that every p-group of class at most $p-1$ is regular. There exists an irregular group of order p^{p+1} and class p, namely, the Sylow p-subgroup of the symmetric permutation group on p^2 symbols. In this group $\Omega_1 < \overline{\Omega}_1$.

More generally, it is known that a p-group G is regular whenever

$$(H_i : \mathfrak{V}_1(H_i)) \leqq p^{p-i}$$

for at least one value of $i = 1, 2, \ldots, p$. G is also regular whenever

$$(\Omega_1 : 1) < p^{p-1}.$$

3. It may be remarked in conclusion that the theory of classification described in the author's first paper in this issue may be generalized by replacing the word $x^{-1}y^{-1}xy$ by an arbitrary word f in any number of letters, or even by an arbitrary system of words. The place of commutator subgroup and central will then be taken by the verbal and marginal subgroups corresponding to f, or (for a system of words) by the join and meet of the corresponding systems of verbal and marginal subgroups, respectively. In this way, we obtain a distinct system of classification corresponding to every fully invariant subgroup of the free group with a denumerably infinite number of generators. Corresponding to the notion of isoclinic groups in the special case, we have an exactly analogous definition of *isologic groups*. And many, but not all, of the theorems of the special theory will be found to carry over into the general theory.

[1]) Not published.

Eingegangen 1. Juli 1939.

Zusammenhang zwischen Potenzbildung und Kommutatorbildung.

Von *O. Grün* in Berlin.

Bekanntlich hat *Burnside*[1]) die Frage aufgeworfen: Erhält man stets eine endliche Gruppe, wenn man in einer freien Gruppe $\mathfrak{F}$, die aus endlich vielen Elementen erzeugt wird, alle m-ten Potenzen von Elementen gleich 1 setzt, wobei m eine natürliche Zahl sei. Diese Frage ist bisher nur für $m = 2, 3, 4$ allgemein beantwortet worden[2]). Die Bearbeitung dieses Problemes, insbesondere für den Fall $m =$ Primzahlpotenz p^i, führt auf die Frage nach dem Zusammenhang zwischen Potenzbildung und Kommutatorbildung; es entsteht die Aufgabe, die als Produkte von p^i-ten Potenzen darstellbaren höheren Kommutatoren zu charakterisieren.

Es wird darauf ankommen, möglichst allgemeine derartige Beziehungen aufzustellen; ein wesentliches Hilfsmittel hierfür bietet die Theorie der Dimensionsgruppen von *Magnus*[3]). Die ganze Untersuchung des § 1 stützt sich auf diese Theorie. Eine hier immer wiederkehrende Anwendung des Hauptsatzes dieser Theorie ist diese: Sei $\mathfrak{G}$ eine Gruppe mit den Elementen $1, S, T, \ldots$ und der absteigenden Zentrenreihe

$$\mathfrak{G}_1 = \mathfrak{G}, \mathfrak{G}_2, \mathfrak{G}_3, \ldots,$$

ferner $\mathfrak{L}$ das aus allen $S - 1, T - 1, \ldots$ im Gruppenring $\mathfrak{R}$ von $\mathfrak{G}$ erzeugte Primideal. Wenn dann für ein Element $G \in \mathfrak{G}$ gezeigt werden kann: $G \equiv 1(\mathfrak{L}^n)$, so folgt $G \in \mathfrak{G}_n$. Der Hilfssatz 1 ermöglicht die Anwendung dieses Satzes auf unser Problem. Legen wir zunächst einige Bezeichnungen fest: In jeder Gruppe $\mathfrak{F}, \mathfrak{G}, \ldots$ sei

$\mathfrak{F}_n, \mathfrak{G}_n, \ldots$ die n-te Untergruppe der absteigenden Zentrenreihe, $\mathfrak{F}_1 = \mathfrak{F}, \mathfrak{G}_1 = \mathfrak{G}, \ldots$

$\mathfrak{F}^k, \mathfrak{G}^k, \ldots$ die $(k-1)$-te Ableitung, $\mathfrak{F}^1 = \mathfrak{F}, \mathfrak{G}^1 = \mathfrak{G}, \ldots$

$\mathfrak{F}(m), \mathfrak{G}(m), \ldots$ für jede natürliche Zahl m diejenige Untergruppe von $\mathfrak{F}, \mathfrak{G}$, die von den m-ten Potenzen aller Elemente aus $\mathfrak{F}, \mathfrak{G} \ldots$ erzeugt wird.

Die Vermutung von Burnside, daß für endliche m und endliche Anzahl der Erzeugenden jede Gruppe $\mathfrak{F}/\mathfrak{F}(m)$ endlich sein müsse, ist dann für den Fall, daß m gleich einer Primzahlpotenz p^i ist, äquivalent mit der Vermutung: „Ist $\mathfrak{F}$ eine freie, etwa von λ unabhängigen Elementen erzeugte Gruppe, so gibt es einen endlichen nur von λ und p^i abhängigen Index n derart, daß $\mathfrak{F}_n < \mathfrak{F}(p^i)$ ist, d. h. daß sich jedes Element

---

[1]) W. Burnside, On an unsettled question in the theory of discontinuous groups, Quarterly Journ. of Math. **33** (1902), 230—238.

[2]) Für $m = 2$ siehe gleich anschließend im Text. Für $m = 3$ siehe *F. Levi-B. L. van der Waerden*, Über eine besondere Klasse von Gruppen, Abh. Math. Sem. Hamburg **9** (1933), 154—158. Für $m = 4$ siehe I. A. de Séguier, Théorie des groupes finis, Bd. **1** (Paris 1904), 72—74.

[3]) W. Magnus, Beziehungen zwischen Gruppen und Idealen in einem speziellen Ring, Math. Ann. **111** (1935), 259—280.

$(t_1, t_2, \ldots, t_n)$ aus $\mathfrak{F}_n$ in der Form $(t_1, t_2, \ldots, t_n) = \prod_k x_k^{p^i}$, $x_k \in \mathfrak{F}$ darstellen läßt." Ebenso ist die weitere Vermutung von Burnside, daß für ungerade m jede Gruppe $\mathfrak{F}/\mathfrak{F}(m)$ auflösbar sei, gleichwertig mit der Vermutung: „Ist m eine ungerade Zahl und wird die freie Gruppe $\mathfrak{F}$ von λ Elementen erzeugt, so gibt es einen nur von m und λ abhängigen Index k derart, daß $\mathfrak{F}^k < \mathfrak{F}(m)$, d. h. daß sich jedes Element $(t_1, t_2; t_3, \ldots, t_k) = d_k$ aus $\mathfrak{F}^k$ in der Form $d_k = \prod_q x_q^m$, $x_q \in \mathfrak{F}$ darstellen läßt." So ist z. B. bekannt, daß sich jedes Element aus $\mathfrak{F}_2$ durch 2-te Potenzen ausdrücken läßt:

$$t^{-1}s^{-1}ts = t^{-2}tss^{-2}ts = t^{-2}(ts \cdot s^{-1}s^{-1}t^{-1})^2(ts)^2.$$

Ebenso ist durch die genannte Untersuchung von Levi—van der Waerden bekannt, daß sich jedes Element aus $\mathfrak{F}_4$ durch 3-te Potenzen ausdrücken läßt. Weiter hat Herr Hall festgestellt: Wird $\mathfrak{F}$ aus 2 Elementen erzeugt, so ist $\mathfrak{F}_7 < \mathfrak{F}(5)$. Es sind aber bisher nur wenig allgemeine Resultate in dieser Beziehung erreicht worden. Das eine stammt von Hall und ist die bekannte Identität:

$$(ab)^m = a^m b^m (a,b)^{\binom{m}{2}} C_3^{\binom{m}{3}} \cdots, \qquad C_i \in \mathfrak{F}_i, \ \{a,b\} = \mathfrak{F}.$$

Das andere hat *Zassenhaus*[4]) kürzlich mit Hilfe der Theorie der Lieschen Ringe bewiesen:

a) $$(T, \underbrace{S, S, \ldots, S}_{p-1}) \in \mathfrak{F}_{p+1}\mathfrak{F}(p), \quad \{T, S\} = \mathfrak{F}.$$

Der Zusammenhang des Potenz-Kommutatorproblems mit der Theorie der Lieschen Ringe wird durch die Theorie der Dimensionsgruppen von *Magnus* hergestellt. Die Kenntnis der darauf bezüglichen Resultate aus den Arbeiten von *Magnus*[4])[5]) sowie von *Witt*[6]) wird hier vorausgesetzt. Die Zassenhaussche Beziehung a) reicht viel weiter als man ihrer spezialisierten Form zunächst ansieht. Denn man hat aus ihr für beliebige k:

b) $$(T, \underbrace{S, S \ldots, S}_{p-1}, T_1, T_2, \ldots, T_k) \equiv 1 \ (\mathfrak{F}_{p+1+k}\mathfrak{F}(p)),$$

d. h. wenn $\mathfrak{F}/\mathfrak{F}(p) = \mathfrak{G}$ gesetzt wird, so liegt der Kommutator

$$(T, \underbrace{S, S, \ldots, S}_{p-1}, T_1, T_2, \ldots, T_k)$$

in $\mathfrak{G}_{p+1+k}$, obwohl er formal, d. h. nach seinem Bildungsgesetz, nur in $\mathfrak{G}_{p+k}$ liegt. Nun ist auch

c) $$(T, T_1, \underbrace{S, S, \ldots, S}_{p-1} T_2, \ldots, T_k) \equiv 1 \ (\mathfrak{G}_{p+1+k})$$

$$\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots$$

$$(T, T_1, T_2, \ldots, T_k, \underbrace{S, S, \ldots, S}_{p-1}) \equiv 1 \ (\mathfrak{G}_{p+1+k}),$$

und dies gilt auch für alle Vertauschungen von $T, T_1, \ldots, T_k$; ferner erhält man aus den obigen noch allgemeinere Gleichungen, indem man S durch $S_1^{\alpha_1} S_2^{\alpha_2} \cdots S_m^{\alpha_m}$ ersetzt; es folgt dann:

$$\textit{II}\,(T, \underbrace{S_1, S_1, \ldots, S_1}_{r_1}, \underbrace{S_2, S_2, \ldots, S_2}_{r_2}, \ldots, \underbrace{S_m, S_m, \ldots, S_m}_{r_m}) \equiv 1 \ (\mathfrak{G}_{p+1}),$$

---

[4]) H. Zassenhaus, Über Liesche Ringe mit Primzahlcharakteristik, Abh. Math. Sem. Hamburg **13** (1939), 1—100.

[5]) W. Magnus, Beziehungen zwischen höheren Kommutatoren, dieses Journ. **177** (1937), 105—115.

[6]) E. Witt, Treue Darstellung Liescher Ringe, dieses Journ. **177** (1937), 152—160.

wobei $r_1 + r_2 + \cdots + r_m = p - 1$ eine beliebige additive Zerfällung von $p - 1$ in positive Summanden ist und das Produkt über alle die Elemente und jedes einmal erstreckt wird, die aus $(T, \underbrace{S_1, \ldots, S_1}_{r_1}, \ldots, \underbrace{S_m, \ldots, S_m}_{r_m})$ durch eine beliebige Vertauschung der Reihenfolge mit fest bleibendem T hervorgehen. Die entsprechende Folgerung besteht für die Kommutatoren b) und c), und so entsteht die Frage, ob man nicht für jedes p einen solchen Wert von k finden kann, daß sich durch die linkenSeiten von b) und c), die ja formal Kommutatoren aus $\mathfrak{G}_{p+k}$ sind, jedes Element aus $\mathfrak{G}_{p+k}$ ausdrücken läßt. Diese Frage führt wieder auf die Theorie der Lieschen Ringe. Sie ist nämlich offenbar gleichwertig mit der Frage: Ist in jedem Lieschen Ring $\mathfrak{L}$ mit Primzahlcharakteristik p der Faktorring $\mathfrak{L}/\mathfrak{J}$ nilpotent, wenn $\mathfrak{J}$ das Ideal aus $\mathfrak{L}$ ist, das aus allen Elementen

$$(\ldots(((u \circ v) \circ v) \ldots) \circ v)$$

entsteht? Weiß man von vornherein, daß $\mathfrak{L}$ oder wenigstens $\mathfrak{L}/\mathfrak{J}$ endlichgliedrig ist, so folgt das aus dem von Zassenhaus auch für Liesche Ringe mit Primzahlcharakteristik p als gültig nachgewiesenen Satz von Engel. Aber diese Voraussetzung läßt einen Beweis der obigen Vermutung mit Hilfe des Satzes von Engel nicht zu; wenn freilich gezeigt werden könnte: „Wenn $\mathfrak{L}$ endlichgliedrig ist, gilt $\mathfrak{L}_1^n = 0$, $\mathfrak{L}_1 = \mathfrak{L}/\mathfrak{J}$, wobei n nur von der Anzahl der (multiplikativen) Erzeugenden von $\mathfrak{L}$ und von p, aber nicht von dem als endlich vorausgesetzten Rang von $\mathfrak{L}$ abhängt", dann würde sich daraus offenbar sofort ein Beweis für obige Vermutung ergeben. Wenn nun diese Vermutung bewiesen ist, so folgt $\mathfrak{F}_{p+k} \leq \mathfrak{F}_{p+k+1}\mathfrak{F}(p)$ und daraus: Es ist entweder $\mathfrak{F}_{p+k} \leq \mathfrak{F}(p)$, oder $\mathfrak{F}_{p+k}\mathfrak{F}(p)/\mathfrak{F}(p)$ ist eine aus endlich vielen Elementen erzeugte p-Gruppe von unendlicher Ordnung, in der alle Elemente außer 1 die Ordnung p haben, und die keinen Normalteiler von endlichem Index enthält; jede endliche p-Gruppe $\mathfrak{G}$ mit gleicher Anzahl der Erzeugenden wie $\mathfrak{F}$, in der $\mathfrak{G}(p) = 1$ gilt, wäre Faktorgruppe von $\mathfrak{F}/\mathfrak{F}_{p+k}\mathfrak{F}(p)$; damit hätte man also in $\mathfrak{F}/\mathfrak{F}_{p+k}\mathfrak{F}(p)$ die allgemeine endliche p-Gruppe, und es wäre die Beschränkung der möglichen Länge der absteigenden Zentrenreihe usw. durch die Anzahl der Erzeugenden und p erwiesen.

Dies zu beweisen und der entsprechende Beweis für Primzahlpotenzen p^i ist eines der wichtigsten Probleme der Theorie der endlichen p-Gruppen. Von der Lösung dieses Problems sind wir noch weit entfernt. Hier soll eine Vorarbeit dazu geleistet werden, indem ein umfassendes System von Beziehungen zwischen höheren Kommutatoren und Elementen mit Primzahlpotenzexponenten aufgestellt wird. Im ersten Paragraphen wird die Untersuchung auf algebraischem Wege geführt; das Mittel dazu bietet die Theorie der Dimensionsgruppen von *Magnus*[3]). Die Resultate des zweiten Paragraphen werden auf rein gruppentheoretischem Wege erreicht, und hierbei zeigt sich, daß vermutlich auch die vor allem von Zassenhaus mit Erfolg verwendete Theorie der Lieschen Ringe nicht ausreichen dürfte, um die „bestmöglichen" Resultate für p-Gruppen zu erlangen; wir werden dort nämlich gewisse Beziehungen von der Form:

d) $$f(a_1, a_2, \ldots, a_n) \equiv 1 \ (\mathfrak{F}(p^i)\mathfrak{F}_{n+\varkappa})$$

erhalten, wobei $f(a_1, a_2, \ldots, a_n)$ ein Kommutator ist, der formal in $\mathfrak{F}_n$ liegt, während $\varkappa$ beliebig aber endlich ist. Gerade die Tatsache, daß $\varkappa > 1$ gewählt werden kann, ergibt die vielleicht später entscheidenden Beziehungen; diese Tatsache kann aber bei der Behandlung im Lieschen Ring aus folgendem Grunde nicht verwertet werden:

e) in der Gruppe ist $(a, bc) = (a, c)\,(a, b)\,(a, b, c)$.

Die geeignete Anwendung dieser Formel auf d) führt dann gerade zu den wichtigsten Gleichungen. e) findet aber kein Äquivalent im Lieschen Ring; dort hat man statt dessen $a \circ (b + c) = a \circ b + a \circ c$, was nur $(a, bc) \equiv (a, c)\,(a, b) \bmod \mathfrak{U}_3$, $\mathfrak{U} = \{a, b\}$ entspricht.

Von besonderer Bedeutung für unser Problem sind die Wittschen Formeln[6]) für den Rang von $\mathfrak{F}_n/\mathfrak{F}_{n+1}$ und ähnliche Rangzahlen; denn wenn für irgendein n $\mathfrak{F}_n < \mathfrak{F}_{n+1}\mathfrak{F}(p^i)$ sein soll, so muß die Anzahl der Basiselemente von $\mathfrak{F}_n$ mod $\mathfrak{F}_{n+1}$, die man durch p^i-te Potenzen bis auf Elemente aus $\mathfrak{F}_{n+1}$ ausdrücken kann, gleich dem Rang von $\mathfrak{F}_n/\mathfrak{F}_{n+1}$ sein, und wenn dies der Fall ist, so ist auch $\mathfrak{F}_n < \mathfrak{F}_{n+1}\mathfrak{F}(p^i)$. Ferner gestatten die Wittschen Formeln eine allerdings sehr hohe Grenze n_k für jedes k derart anzugeben, daß $\mathfrak{F}_{n_k} < \mathfrak{F}^k\mathfrak{F}(p^i)$, d. h. daß in einer p-Gruppe $\mathfrak{G}$ mit $\mathfrak{G}(p^i) = 1$, jedenfalls $\mathfrak{G}_{n_k} < \mathfrak{G}^k$ ist. (Für freie Gruppen $\mathfrak{F}$ gibt es bekanntlich keine derartige Grenze, wenn $k > 2$ ist, d. h. für jeden beliebigen Index n gibt es Elemente aus $\mathfrak{F}_n$, die nicht in der 2-ten Ableitung von $\mathfrak{F}$ liegen.)

§ 1.

Von jetzt an gelte durchweg:

Soweit Ringe oder Ideale eingeführt werden, sei stets als Koeffizientenbereich der Ring der rationalen mod p ganzen Zahlen gewählt; p sei stets ungerade Primzahl.

$\mathfrak{G}$ sei durchweg eine aus endlich vielen Elementen erzeugte Gruppe, in der gelte:

$$\mathfrak{G}(p^i) = \{\ldots, S^{p^i}, \ldots\} = 1, \quad S \in \mathfrak{G}.$$

$\mathfrak{R}$ sei der Gruppenring von $\mathfrak{G}$, $\mathfrak{L}$ das aus allen $S - 1$ ($S \in \mathfrak{G}$, 1 das Einselement von $\mathfrak{G}$), erzeugte zweiseitige Ideal in $\mathfrak{R}$. Wird $\mathfrak{G}$ etwa aus λ Elementen $T_i = 1 + u_i$ erzeugt, $i = 1, 2, \ldots, \lambda$, so wird $\mathfrak{L}$ aus den u_i multiplikativ erzeugt.

Hilfssatz 1. *Wenn $\mathfrak{R}$ auf $\mathfrak{R}/p^i\mathfrak{L}$ abgebildet wird, so ist das Bild von $\mathfrak{G}$ isomorph mit $\mathfrak{G}$. Es werde hierbei vorausgesetzt, daß für irgendeine beliebig große aber endliche Zahl q gelte:* $\mathfrak{G}_q = 1$.

Beweis. Zunächst ist $\mathfrak{G}$ bei unserer Annahme von endlicher Ordnung, der Gruppenring $\mathfrak{R}$ hat also endlichen Rang. Die Abbildung von $\mathfrak{R}$ auf $\mathfrak{R}/p^i\mathfrak{L}$ erfolgt dadurch, daß man jedem Element $a \in \mathfrak{R}$ das Element $a + p^i\mathfrak{L}$ zuordnet.

(1) Die Abbildung von $\mathfrak{G}$ ist isomorph. Denn sei S ein Element aus $\mathfrak{G}_n$ aus einer (von $\mathfrak{G}_{n+1}$ verschiedenen) Restklasse von $\mathfrak{G}_{n+1}$, das auf ein Element aus $\mathfrak{G}_{n+1}$ abgebildet wird, $n = 1, 2, \ldots$. Dann hat S die Form $1 + L_n + L_{n+1} + \cdots$, wobei L_n, $L_{n+1}, \ldots$ Restklassenelemente von $\mathfrak{L}^n/\mathfrak{L}^{n+1}$, $\mathfrak{L}^{n+1}/\mathfrak{L}^{n+2}, \ldots$ sind und $L_n \neq 0$ ist. Sei $T = 1 + L'_{n+1} + \cdots$ das Element aus $\mathfrak{G}_{n+1}$, auf das S abgebildet wird. Dann muß

$$1 + L_n + L_{n+1} + \cdots \equiv 1 + L'_{n+1} + \cdots \,(p^i\mathfrak{L})$$

sein. Daraus folgt $L_n \equiv 0\ (p^i\mathfrak{L})$, also muß $L_n = p^iL''_n$ sein, wobei wieder $L''_n \neq 0$ aus einer Restklasse von $\mathfrak{L}^n/\mathfrak{L}^{n+1}$ stammt. Sind nun $S_k - 1 = u_k$, $k = 1, 2, \ldots$ die multiplikativen Erzeugenden von $\mathfrak{L}$ und ist Λ der durch die Multiplikationsvorschrift $u_i \circ u_k = u_iu_k - u_ku_i$ aus ihnen entstehende Liesche Ring, so ist L_n ein Element aus Λ^n aus einer Restklasse von Λ^{n+1}; sei $l_1, l_2, \ldots$ eine Basis von Λ^n/Λ^{n+1} und etwa $L_n = \sum_k \alpha_k l_k$; damit $L_n = p^iL''_n$ sein kann, muß $\alpha_k \equiv 0\ (p^i)$, d. h. $\alpha_k = p^i\beta_k$ sein (Magnus[5])), also $S = 1 + p^i \sum_k \beta_k l_k + L_{n+1}$; nun existieren in $\mathfrak{G}_n$ die Elemente $T_k \equiv 1 + l_k \bmod \mathfrak{L}^{n+1}$, also $T_k^{\beta_k} \equiv 1 + \beta_k l_k\ (\mathfrak{L}^{n+2})$, $k = 1, 2, \ldots$. Daher wird $S(\Pi T_k^{-\beta_k})^{p^i} = 1 + L'''_{n+1}$, $L'''_{n+1} \in \mathfrak{L}^{n+1}$, und wegen $\mathfrak{G}(p^i) = 1$ heißt das: $S \in \mathfrak{G}_{n+1}$, gegen die Voraussetzung, daß S aus einer Restklasse von $\mathfrak{G}_{n+1}$

stamme; die Annahme, daß $S \in \mathfrak{G}_n$ auf ein Element aus $\mathfrak{G}_{n+1}$ abgebildet werde, führt also zu einem Widerspruch. Demnach kann auch kein von 1 verschiedenes Element auf 1 abgebildet werden.

(2) Es gilt auch für das Bild von $\mathfrak{G}$ der Satz von den Dimensionsgruppen. Angenommen, ein Element S aus $\mathfrak{G}_n$ aus einer Restklasse von $\mathfrak{G}_{n+1}$ habe in der Abbildung die Dimenison $n+1$. Das würde offenbar bedeuten:

$$S = 1 + L_n + L_{n+1} \equiv 1 + L'_{n+1} + \cdots (p^i \mathfrak{L}),$$

also wieder $L_n = p^i L'_n$, und es folgt wie vorher $S \in \mathfrak{G}_{n+1}$ gegen die Voraussetzung.

Nunmehr werde unter $\mathfrak{G}$ das Bild der ursprünglichen Gruppe $\mathfrak{G}$ auf $\mathfrak{R}/p^i\mathfrak{L}$ verstanden und für $\mathfrak{R}/p^i\mathfrak{L}$ wieder $\mathfrak{R}$, sowie für $\mathfrak{L}/p^i\mathfrak{L}$ wieder $\mathfrak{L}$ geschrieben. Wegen Hilfssatz 1 gelten alle für das Bild von $\mathfrak{G}$ bewiesenen gruppentheoretischen Resultate auch für die ursprüngliche Gruppe $\mathfrak{G}$.

Aus Hilfssatz 1 ergibt sich übrigens ohne weitere Rechnung die Folgerung:

$$(T_1^{p^{\nu_1}}, T_2^{p^{\nu_2}}, \ldots, T_k^{p^{\nu_k}})^{p^\mu} \equiv 1 \ (\mathfrak{U}_{k+1}),$$

wo $\mathfrak{U} = \{T_1, \ldots, T_k\}$ und $\nu_1 + \nu_2 + \cdots + \nu_k + \mu \geqq i$ ist.

Hilfssatz 2. *Ist $S = 1 + u$ ein beliebiges Element von $\mathfrak{G}$ und $i < p$, sowie $\mathfrak{L}_1$ der Teilring (u), so ist*

$$(1\,a) \qquad p^{i-1} u^{p^\varkappa} \equiv 0 \ (\mathfrak{L}_1^{p^{\varkappa+1}}), \qquad \varkappa = 1, 2, \ldots, i$$

$$(1\,b) \qquad p^{i-2} u^{2p^\varkappa - p^{\varkappa-1}} \equiv 0 \ (\mathfrak{L}_1^{p^{\varkappa+1}}), \qquad \varkappa = 2, 3, \ldots, i+1$$

$$(1\,c) \qquad p^{i-3} u^{3p^\varkappa - 2p^{\varkappa-1}} \equiv 0 \ (\mathfrak{L}_1^{p^{\varkappa+1}}), \qquad \varkappa = 3, 4, \ldots, i+2$$

. . . . . .

$$(1\,d) \quad p^{i-\nu} u^{\nu p^\varkappa - (\nu-1)p^{\varkappa-1}} \equiv 0 \ (\mathfrak{L}_1^{p^{\varkappa+1}}), \quad \varkappa = \nu, \nu+1, \ldots, i+\nu-1; \ \nu = 1, 2, \ldots, i.$$

Ferner gelten diese Gleichungen bei beliebigen i für $\nu < p$.

Beweis. Aus $S^{p^i} = 1 = (1+u)^{p^i}$ folgt wegen $p^i\mathfrak{L} = 0$:

$$(2) \qquad \sum_{k=1}^{p^{i-1}} \binom{p^i}{pk} u^{pk} = 0.$$

Setzen wir $\binom{p^i}{p} u^p + \binom{p^i}{2p} u^{2p} + \cdots + \binom{p^i}{(p-1)p} u^{(p-1)p} = \binom{p^i}{p} u^p (1+x)$, so ist x ganz. Die Multiplikation mit $1 - x + x^2 - x^3 + \cdots + x^{p-1}$ ergibt

$$\left(\sum_{k=1}^{p^{i-1}} \binom{p^i}{pk} u^{pk}\right)(1 - x + x^2 - \cdots + x^{p-1}) = \binom{p^i}{p} u^p + u^{p^2} L,$$

wobei L ein Ausdruck $\alpha_0 + \alpha_1 u^p + \cdots$ ist mit für p ganzen $\alpha_0, \alpha_1, \ldots$. Das ergibt

$$p^{i-1} u^p \equiv 0 \ (\mathfrak{L}_1^{p^2}),$$

die erste der Gleichungen (1a). Multipliziert man aber (2) mit p, so werden alle Terme mit Koeffizienten $\binom{p^i}{pk}$, $(p, k) = 1$, annulliert, denn $p\binom{p^i}{pk} \equiv 0 \bmod p^i$, wenn $(k, p) = 1$. Es wird also

$$(3) \qquad p \sum_{(k,p)=1} \binom{p^i}{pk} u^{pk} = 0$$

$$= p\binom{p^i}{p^2} u^{p^2} + p\binom{p^i}{2p^2} u^{2p^2} + \cdots + p\binom{p^i}{(p-1)p^2} u^{(p-1)p^2} + L_1^{(p^2)}, \ L_1^{(p^2)} \in \mathfrak{L}_1^{p^2}.$$

Setzt man nunmehr $p\sum_{k=1}^{p-1}\binom{p^i}{p^2k}u^{p^2k} = p\binom{p^i}{p^2}u^{p^2}(1+x)$, so ist wieder x ganz, und es folgt durch Multiplikation von (3) mit $1 - x + x^2 - \cdots + x^{p-1}$:

$$p^{i-1}u^{p^2} \equiv 0\ (\mathfrak{Q}_1^{p^3}),$$

d. i. die zweite der Gleichungen (1a). Ebenso ergibt sich die nächste durch Multiplikation von (2) mit p^2 und entsprechende Behandlung wie oben, usw. Damit sind die Gleichungen (1a) bewiesen.

Die Gleichungen (1b) folgen nun, indem man (2) mit u^{p^2-p}, $pu^{p^2-p^2}$, $p^2u^{p^4-p^3}$, ... multipliziert und die schon bewiesenen Gleichungen (1a) berücksichtigt. Dies möge nur noch für die erste Gleichung (1b) durchgeführt werden:

$$\left(\sum_{k=1}^{p^{i-1}}\binom{p^i}{pk}u^{pk}\right)u^{p^2-p} = \sum_{k=1}^{p^{i-1}}\binom{p^i}{pk}u^{p^2+(k-1)p} = 0. \tag{4}$$

Nach Gleichung (1a) ist $p^{i-1}u^{p^2} \equiv 0\ (\mathfrak{Q}_1^{p^3})$; daher ergibt (4)

$$\binom{p^i}{p^2}u^{2p^2-p} + \binom{p^i}{2p^2}u^{3p^2-p} + \cdots \equiv 0\ (\mathfrak{Q}_1^{p^3}).$$

Daraus folgt wieder wie oben

$$p^{i-2}u^{2p^2-p} \equiv 0\ (\mathfrak{Q}_1^{p^3}).$$

Ebenso erhält man die Gleichung (1c), indem man (2) mit $u^{2p^3-2p^2}$, $pu^{2p^4-2p^3}$, ... multipliziert und entsprechend wie oben verfährt; und auf gleiche Weise folgen durch Multiplikation von (2) mit $u^{(\nu-1)p^\nu-(\nu-1)p^{\nu-1}}$, $pu^{(\nu-1)p^{\nu+1}-(\nu-1)p^\nu}$, ... und Heranziehung der bereits bewiesenen Gleichungen die allgemeinen Gleichungen (1d).

Versteht man für beliebige $T, S \in \mathfrak{G}$ unter (T, S, n) den Kommutator

$$(T, \underbrace{S, S, \ldots, S}_{n}),\quad n = 1, 2, \ldots,$$

und ist $\mathfrak{U}$ die Untergruppe $\{T, S\}$, so ergeben die Gleichungen (1) sofort

Satz 1.

$$(T, S, 2\nu p^\nu - 2(\nu-1)p^{\nu-1} - 1)^{p^{i-\nu}} \equiv 1\ (\mathfrak{U}_{2\nu p^\nu-2(\nu-1)p^{\nu-1}+1}), \tag{5}$$
$$\nu = 1, 2, \ldots, \min(p, i).$$

Beweis. Ist $T = 1 + v$, $S = 1 + u$, so ist zu beweisen:

$$p^{i-\nu}(\underbrace{(\ldots((v \circ u) \circ u)\ldots) \circ u}_{2\nu p^\nu - 2(\nu-1)p^{\nu-1} - 1}) \equiv 0\ (\mathfrak{Q}_{\mathfrak{U}}^{2\nu p^\nu-2(\nu-1)p^{\nu-1}+1}),$$

wobei $\mathfrak{Q}_{\mathfrak{U}}$ der in $\mathfrak{Q}$ aus v und u entstehende Teilring und $u \circ v = uv - vu$ ist. Nun ist für beliebige n

$$(\underbrace{(\cdots((v \circ u) \circ u)\cdots) \circ u}_{n}) = \sum_{k=0}^{n}(-1)^k\binom{n}{k}u^k vu^{n-k}.$$

Setzt man $n = 2\nu p^\nu - 2(\nu-1)p^{\nu-1} - 1$, so ist in jedem einzelnen Summanden $\binom{n}{k}u^k vu^{n-k}$ entweder k oder $n - k \geqq \nu p^\nu - (\nu-1)p^{\nu-1}$, also entweder $p^{i-\nu}u^k$ oder $p^{i-\nu}u^{n-k} \in \mathfrak{Q}_1^{p^{\nu+1}} < \mathfrak{Q}_{\mathfrak{U}}^{p^{\nu+1}}$; der ganze Summand liegt also in

$$\mathfrak{Q}_{\mathfrak{U}}^{p^{\nu+1}+\nu p^\nu-(\nu-1)p^{\nu-1}} < \mathfrak{Q}_{\mathfrak{U}}^{2\nu p^\nu-(\nu-1)p^{\nu-1}+1} < \mathfrak{Q}_{\mathfrak{U}}^{2\nu p^\nu-2(\nu-1)p^{\nu-1}+1},$$

w. z. b. w. Die Kommutatoren (5), die formal, d. h. nach ihrem Bildungsgesetz, in $\mathfrak{U}_{2vp^v-2(v-1)p^{v-1}}$ liegen, sind also tatsächlich Elemente einer Untergruppe der absteigenden Zentrenreihe von $\mathfrak{U}$ mit einem um 1 höheren Index. Aus (5) erhält man einerseits durch die Substitution $S = \prod_k S_k^{\alpha_k}$ Beziehungen von der Form:

$$\Pi'\Pi\,(T, \underbrace{S_1, \ldots, S_1}_{r_1}, \underbrace{S_2, \ldots, S_2}_{r_2}, \ldots, \underbrace{S_q, \ldots, S_q}_{r_q})^{p^{i-v}} \equiv 1\,(\mathfrak{U}_{2vp^v-2(v-1)p^{v-1}+1}),$$

wenn $\{T, S_1, \ldots, S_q\} = \mathfrak{U}$ und $r_1 + r_2 + \cdots + r_q = 2vp^v - 2(v-1)p^{v-1} - 1$

ist und das Produkt Π über alle verschiedenen Elemente, jedes einmal, erstreckt wird, die aus $(T, \underbrace{S_1, \ldots, S_1}_{r_1}, \underbrace{S_2, \ldots, S_2}_{r_2}, \ldots, \underbrace{S_q, \ldots, S_q}_{r_q})$ durch irgendeine Vertauschung beliebig vieler $S_1, S_2, \ldots, S_q$ hervorgehen, so daß in Π z. B. auch das Element

$$(T, S_2, \underbrace{S_1, \ldots, S_1}_{r_1-1}, S_2, S_1, \underbrace{S_2, \ldots, S_2}_{r_2-1}, \ldots)$$

vorkommt, während Π' über $r_1, r_1 + p^{v-1}(p-1), \ldots$ erstreckt wird. Speziell, wenn $n = 2vp^v - 2(v-1)\,p^{v-1} - 1$ gesetzt wird:

$$\Pi(T, S_1, S_2, \ldots, S_n)^{p^{i-v}} \equiv 1\,(\mathfrak{U}_{n+2}).$$

Andererseits erhält man aus (5) auch durch weitere Kommutatorbildung:

$$(T, \underbrace{S, \ldots, S}_{n}, T_1, T_2, \ldots, T_q)^{p^{i-v}} \equiv 1\,(\mathfrak{U}_{n+q+2}),$$

wenn $\{T, S, T_1, T_2, \ldots, T_q\} = \mathfrak{U}$, ebenso

$$(T, T_1, \underbrace{S, \ldots, S}_{n}, T_2, \ldots, T_q)^{p^{i-v}} \equiv 1\,(\mathfrak{U}_{n+q+2})$$

$$\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots$$

$$(T, T_1, \ldots, T_q, \underbrace{S, \ldots, S}_{n})^{p^{i-v}} \equiv 1\,(\mathfrak{U}_{n+q+2}).$$

Es folgt nunmehr aus dem bekannten *Hall*schen Satz[7]): Ist R ein beliebiges Element aus der Untergruppe $\mathfrak{U}_{v,q}$ von $\mathfrak{G}$, die aus allen Kommutatoren

$$(T, \underbrace{S, \ldots, S}_{n_v}, T_1, T_2, \ldots, T_q), \ldots, (T, T_1, \ldots, T_q, \underbrace{S, \ldots, S}_{n_v}), \quad n_v = 2vp^v - 2(v-1)p^{v-1} - 1,$$

entsteht, wobei $T, S, T_1, T_2, \ldots, T_q$ alle Elemente von $\mathfrak{G}$ durchlaufen, so ist $R^{p^{i-v}} \equiv 1\,(\mathfrak{G}_{n_v+q+2})$, d. h. es ist $\mathfrak{U}_{v,q}\,\mathfrak{G}_{n_v+q+2}/\mathfrak{G}_{n_v+q+2}$ höchstens vom Typus $(p^{i-v}, p^{i-v}, \ldots, p^{i-v})$, wobei $\mathfrak{G}_{n_{v-1}} < \mathfrak{U}_{v,q}$ ist. Speziell: wenn es ein solches q gibt, daß $\mathfrak{U}_{v,q}\,\mathfrak{G}_{n_v+q+2} = \mathfrak{G}_{n_v+q+1}$ ist, so ist $\mathfrak{G}_{n_v+q+1}/\mathfrak{G}_{n_v+q+2}$ höchstens vom Typus $(p^{i-v}, p^{i-v}, \ldots, p^{i-v})$. Es gibt aber einen solchen Index q sicher dann, wenn in dem mit den Elementen von $\mathfrak{G}$ und dem Ring der rationalen mod p ganzen Zahlen als Koeffizientenbereich durch eine entsprechende Multiplikationsvorschrift $u \circ v = uv - vu$ gebildeten Lieschen Ring $\mathfrak{L}$ gilt: $\mathfrak{J}$ sei das aus allen $u \circ v^{n_v}$ in $\mathfrak{L}$ entstehende Ideal[8]); der Faktorring $\mathfrak{L}/\mathfrak{J} = \mathfrak{L}_1$ ist nilpotent, und es ist $\mathfrak{L}_1^{n_v+q+1} = 0$; d. h. wenn in $\mathfrak{L}$ der Engelsche Satz wenigstens mit dem Exponenten n_v gilt.

---

[7]) P. Hall, A contribution to the theory of groups of prime-power order, Proc. London Math. Soc. (2) **36** (1934), 64, Theorem (3. 2).

[8]) Unter $u \circ v^n$ sei die Bildung $((\ldots((u \circ v) \circ v)\ldots) \circ v)$ verstanden.

Um Satz 2 zu verallgemeinern und zu verschärfen, müssen wir die Beziehung aus Satz 1 verschärfen. Die nachstehende Rechnung ist etwas ausführlicher, als für das hier gesuchte Resultat erforderlich ist; aber in § 2 werden dieselben Beziehungen in anderer Bedeutung auftreten, und wir werden alsdann das hier abgeleitete genauere Resultat verwenden können.

Die Rechnungsmethode besteht darin, daß zunächst eine Kongruenz für $p^{i-1}u^{p^{\varkappa+1}}$, $\varkappa = 0, 1, \ldots$, festgestellt wird. Mit Hilfe dieser wird dann eine Kongruenz für $p^{i-2}u^{2p^{\varkappa+1}-p^{\varkappa}}$, $\varkappa = 0, 1, \ldots$, gewonnen; diese wird aber nochmals in die rechte Seite der ersten Kongruenz eingeführt, wodurch die erste Kongruenz verschärft wird. Dann wird die zweite Kongruenz weiter benutzt, um eine Kongruenz für $p^{i-3}u^{3p^{\varkappa+1}-2p^{\varkappa}}$ zu berechnen, die dann wieder in die rechten Seiten von (1) und (2) eingeführt wird, usw.

Hilfssatz 3. *Sei $S = 1 + u$ ein Element aus $\mathfrak{G}$ und $\mathfrak{L}_1$ der aus u entstehende Teilring. Dann gilt*

1) *für alle* $0 \leqq \varkappa \leqq i-1$

$$(6) \qquad p^{i-\nu}u^{p^{\varkappa}(\nu p-\nu+1)} \equiv 0 \left(\sum_{\mu=\varkappa+2}^{i} p^{i-\mu}\mathfrak{L}_1^{p^{\mu}}\right)\mathfrak{L}_1^{(\varkappa+1-\nu)p^{\varkappa+1}(p-1)+(\nu-1)p^{\varkappa}(p-1)},$$

$$\nu = 1, 2, \ldots, \varkappa+1,$$

2) $$p^{i-\nu}u^{\nu p^i-(\nu-1)p^{i-1}} = 0, \qquad \nu = 1, 2, \ldots, i.$$

Beweis. Es ist

$$\sum_{k=1}^{p^{i-1}} \binom{p^i}{pk} u^{pk} = 0.$$

Daraus ergibt sich zunächst (6. 2) so:

$$\alpha) \qquad p^{i-1}\sum_{k=1}^{p^{i-1}} \binom{p^i}{pk} u^{pk} = 0 = p^{i-1}u^{p^i}.$$

$$\beta) \qquad p^{i-2}u^{p^i-p^{i-1}}\sum_{k=1}^{p^{i-1}} \binom{p^i}{pk} u^{pk} = 0$$

$$= p^{i-2}\sum_{k=1}^{p-1} \binom{p^i}{p^{i-1}k} u^{p^{i-1}k+p^i-p^{i-1}} + p^{i-2}u^{2p^i-p^{i-1}} = p^{i-2}u^{2p^i-p^{i-1}} \text{ wegen } \alpha).$$

Sei $p^{i-\nu}u^{\nu p^i-(\nu-1)p^{i-1}} = 0$ für $\nu = 1, 2, \ldots, \nu_1$ schon bewiesen.

Dann wird

$$p^{i-\nu_1-1}u^{\nu_1 p^i-\nu_1 p^{i-1}}\sum_{k=1}^{p^{i-1}} \binom{p^i}{pk} u^{pk} = 0 = p^{i-\nu_1-1}\sum_{k=1}^{p^{\nu_1}} \binom{p^i}{p^{i-\nu_1}k} u^{p^{i-\nu_1}k+\nu_1 p^i-\nu_1 p^{i-1}}.$$

Auf Grund der Induktionsvoraussetzung wird nun für $k = 1, 2, \ldots, p^{\nu_1}-1$ jeder Summand

$$p^{i-\nu_1-1}\binom{p^i}{p^{i-\nu_1}k} u^{p^{i-\nu_1}k+\nu_1 p^i-\nu_1 p^{i-1}} = 0.$$

Sei nämlich k genau durch p^s teilbar. Dann ist $\binom{p^i}{pk}$ genau durch p^{i-s-1} teilbar. Es wird also

$$p^{i-\nu_1-1}u^{\nu_1 p^i-\nu_1 p^{i-1}}\binom{p^i}{pk}u^{pk} = p^{2i-\nu_1-s-2}gu^{pk+\nu_1 p^i-\nu_1 p^{i-1}}$$

mit ganzem g. Wenn nun $2i - \nu_1 - s - 2 \geqq i - \nu_1$ ist, ist dieser Ausdruck auf Grund der Induktionsvoraussetzung gleich 0. Die Ungleichung $2i - \nu_1 - s - 2 \geqq i - \nu_1$ bedeutet nun $s \leqq i - 2$. Das ist aber für alle k in $\binom{p^i}{pk}$ der Fall, außer für $k = p^{i-1}$.

Aus der damit bewiesenen Beziehung folgt dann auch für den letzten Summanden

$$p^{i-\nu_1-1}\, u^{(\nu_1+1)p^i-\nu_1 p^{i-1}} = 0.$$

Damit ist (6. 2) bewiesen.

(6. 1) folgt so:

A. Es ist zunächst

$$p^\varkappa \sum_{k=1}^{p^i} \binom{p^i}{k} u^k = 0 = p^\varkappa \sum_{k=p^\varkappa}^{p^{i-1}} \binom{p^i}{pk} u^{pk} = p^{i-1}\, u^{p^{\varkappa+1}}\, x_1 + p^{i-2}\, u^{p^{\varkappa+2}}\, x_2 + \cdots + p^\varkappa\, u^{p^i} = 0,$$

wobei

$$x_1 = \frac{1}{p^{i-\varkappa-1}} \left(\binom{p^i}{p^{\varkappa+1}} + \binom{p^i}{2p^{\varkappa+1}} u^{p^{\varkappa+1}} + \cdots + \binom{p^i}{rp^{\varkappa+1}} u^{(r-1)p^{\varkappa+1}} + \cdots \right),$$

$$(r, p) = 1, \quad r = 1, 2, \ldots,$$

x_1 ganz für p, ebenso $x_2, \ldots$ Setzt man noch $x_1 = \binom{p^i - 1}{p^{\varkappa+1} - 1}(1 + y_1)$, so wird auch y_1 ganz für p und durch Multiplikation mit $1 - y_1 + y_1^2 - y_1^3 + \cdots$ folgt

$$1\alpha) \qquad p^{i-1}\, u^{p^{\varkappa+1}} \equiv 0 \left(\sum_{\mu=2}^{i-\varkappa} p^{i-\mu}\, \mathfrak{Q}_1^{p^{\varkappa+\mu}} \right).$$

B. Es ist weiter

$$p^{\varkappa-1}\, u^{p^\varkappa(p-1)} \sum_{k=1}^{p^i} \binom{p^i}{k} u^k = 0$$

$$= p^{\varkappa-1}\, u^{p^\varkappa(p-1)} \sum_{k=1}^{p^{i-\varkappa}} \binom{p^i}{p^\varkappa k} u^{p^\varkappa k}$$

$$= (p^{i-1}\, u^{p^\varkappa}\, x_1 + p^{i-2}\, u^{p^{\varkappa+1}}\, x_2 + \cdots)\, u^{p^\varkappa(p-1)},$$

wobei $x_1, x_2, \ldots$ ganz für p und von der Form $\alpha_1 + \beta_1 L_1^{p^\varkappa}$, $\alpha_2 + \beta_2 L_2^{p^{\varkappa+1}}, \ldots$ sind, mit $L_1, L_2, \ldots \in \mathfrak{Q}_1$ und $\alpha_1, \alpha_2, \ldots \not\equiv 0\ (p)$. Dies ergibt

$$p^{i-2}\, u^{p^\varkappa(2p-1)}\, x_2 \equiv 0 \left(p^{i-1}\, \mathfrak{Q}_1^{p^{\varkappa+1}} + \sum_{\mu=3}^{i-\varkappa+1} p^{i-\mu}\, \mathfrak{Q}_1^{p^{\varkappa-1+\mu}} \right) \mathfrak{Q}_1^{p^\varkappa(p-1)}.$$

Führt man in dem Ideal rechts die Kongruenz $1\alpha)$ ein und eliminiert x_2 wie oben, so folgt

$$p^{i-1}\, u^{p^\varkappa(2p-1)} \equiv 0 \left(p^{i-2}\, \mathfrak{Q}_1^{p^{\varkappa+2}} + \sum_{\mu=3}^{i-\varkappa+1} p^{i-\mu}\, \mathfrak{Q}_1^{p^{\varkappa-1+\mu}} \right) \mathfrak{Q}_1^{p^\varkappa(p-1)},$$

und daraus (weil $p^{i-2}\, \mathfrak{Q}_1^{p^\varkappa(2p-1)} > p^{i-2}\, \mathfrak{Q}_2^{p^{\varkappa+2}+p^\varkappa(p-1)}$)

$$2\alpha) \qquad p^{i-1}\, u^{p^\varkappa(2p-1)} \equiv 0 \left(\sum_{\mu=3}^{i-\varkappa+1} p^{i-\mu}\, \mathfrak{Q}_1^{p^{\varkappa-1+\mu}} \right) \mathfrak{Q}_1^{p^\varkappa(p-1)} \qquad (\varkappa \geqq 1)$$

also auch

$$p^{i-2}\, \mathfrak{Q}_1^{p^\varkappa(2p-1)} \equiv 0 \left(\sum_{\mu=3}^{i-\varkappa+1} p^{i-\mu}\, \mathfrak{Q}_1^{p^{\varkappa-1+\mu}} \right) \mathfrak{Q}_1^{p^\varkappa(p-1)}.$$

Dies auf das erste Glied des Ideals rechts in $1\alpha)$ angewendet, ergibt

$$p^{i-1}\, u^{p^{\varkappa+1}} \equiv 0 \left(\sum_{\mu=3}^{i-\varkappa+\mu} p^{i-\mu}\, \mathfrak{Q}_1^{p^{\varkappa-1+\mu}+p^\varkappa(p-1)+p^\varkappa(p-1)^2} + \sum_{\mu=3}^{i-\varkappa} p^{i-\mu}\, \mathfrak{Q}_1^{p^{\varkappa+\mu}} \right).$$

Nun ist

$$p^{\varkappa-1+\mu} + p^{\varkappa}(p-1) + p^{\varkappa}(p-1)^2 = p^{\varkappa-1+\mu} + p^{\varkappa+1}(p-1) < p^{\varkappa+\mu} \quad (\mu > 2);$$

damit folgt

$$1\beta) \qquad p^{i-1} u^{p^{\varkappa+1}} \equiv 0 \left(\sum_{\mu=3}^{i-\varkappa+1} p^{i-\mu} \mathfrak{Q}_1^{p^{\varkappa-1+\mu}} \right) \mathfrak{Q}_1^{p^{\varkappa+1}(p-1)} \qquad (\varkappa \geqq 1),$$

also auch

$$p^{i-1} \mathfrak{Q}_1^{p^{\varkappa+1}} \equiv 0 \left(\sum_{\mu=3}^{i-\varkappa+1} p^{i-\mu} \mathfrak{Q}_1^{p^{\varkappa-1+\mu}} \right) \mathfrak{Q}_1^{p^{\varkappa+1}(p-1)}.$$

C. So würde man nacheinander durch Multiplikation von

$$\sum_{k=1}^{p^{i-1}} \binom{p^i}{k} u^k = 0 \quad \text{mit} \quad p^{\varkappa-\nu} u^{\nu p^{\varkappa}(p-1)}, \qquad (\nu = 0, 1, \ldots, \varkappa)$$

und Anwendung auf die schon festgestellten Kongruenzen die Beziehungen (6. 1) finden. Wir können sie jetzt durch vollständige Induktion beweisen. Sie dazu für festes $\varkappa$ und alle $\nu_1 < \nu$ schon bewiesen, daß man aus

$$p^{\varkappa-\nu_1} u^{\nu_1 p^{\varkappa}(p-1)} \sum_{k=1}^{p^i} \binom{p^i}{k} u^k = 0$$

erhält:

$$4) \qquad p^{i-\lambda} u^{p^{\varkappa}(\lambda p-(\lambda-1))} \equiv 0 \left(\sum_{\mu=\nu_1+2}^{i-\varkappa+\nu_1} p^{i-\mu} \mathfrak{Q}_1^{p^{\varkappa-\nu+\mu}} \right) \mathfrak{Q}_1^{(\nu_1+1-\lambda)p^{\varkappa+1}(p-1)+(\lambda-1)^{\varkappa}(p-1)}$$
$$\lambda = 1, 2, \ldots, \nu+1.$$

Die Formeln $1\alpha)$, $1\beta)$, $2\alpha)$ sind von dieser Form für $\nu_1 = 0$, $\lambda = 1$ bzw. $\nu_1 = 1$, $\lambda = 1$ bzw. $\nu_1 = 1$, $\lambda = 2$. Allgemein ist

$$p^{\varkappa-\nu} u^{\nu p^{\varkappa}(p-1)} \sum_{k=1}^{p^i} \binom{p^i}{k} u^k = 0$$

$$= p^{\varkappa-\nu} u^{\nu p^{\varkappa}(p-1)} \sum_{k=1}^{p^{i-\varkappa+\nu-1}} \binom{p^i}{p^{\varkappa-\nu+1} k} u^{p^{\varkappa-\nu+1} k}$$

$$= \left(\sum_{\mu=1}^{i-\varkappa+\nu-1} p^{i-\mu} u^{p^{\varkappa-\nu+\mu}} x_\mu \right) u^{\nu p^{\varkappa}(p-1)},$$

wo die x_μ von der Form $\alpha_\mu + \beta_\mu L_\mu^{p^{\varkappa-\nu+\mu}}$ mit $L_\mu \in \mathfrak{Q}_1$ und $\alpha_\mu \not\equiv 0 \bmod p$ sind. Daraus folgt

$$p^{i-\nu-1} u^{p^{\varkappa}((\nu+1)p-\nu)} \equiv 0 \left(\sum_{\mu+1}^{\nu} p^{i-\lambda} \mathfrak{Q}_1^{p^{\varkappa-\nu+\mu}} \sum_{\mu=\nu-2}^{i-\varkappa+\nu-1} p^{i-\mu} \mathfrak{Q}_1^{p^{\varkappa-\nu+\mu}} \right) \mathfrak{Q}_1^{\nu p^{\varkappa}(p-1)}.$$

Nach 4) ist für $\nu_1 = \nu - 1$ in dem Ideal rechts in der ersten Teilsumme jeder Summand

$$p^{i-\lambda} \mathfrak{Q}_1^{p^{\varkappa-\nu+\lambda}+\nu p^{\varkappa}(p-1)} \equiv 0 \left(\sum_{\mu=\nu_1+1}^{i-\varkappa+\nu_1} p^{i-\mu} \mathfrak{Q}_1^{p^{\varkappa-\nu_1+\mu}} \right) \mathfrak{Q}_1^{\beta+(\nu_1+1-\lambda)p^{\varkappa+1}(p-1)+(\lambda-1)p^{\varkappa}(p-1)}.$$

wobei

$$\beta = p^{\varkappa-\nu+\lambda} + p^{\varkappa}((\nu-\lambda)\, p - (\nu - \lambda + 1)).$$

Für $\lambda = \nu$ wird $\beta = p^{\varkappa} - p^{\varkappa} = 0$; für $\lambda < \nu$ aber $\beta > 0$. Daher folgt

$$5a) \qquad p^{i-\nu-1} u^{p^{\varkappa}((\nu+1)p-\nu)} \equiv 0 \left(\sum_{\mu=\nu+2}^{i-\varkappa+\nu} p^{i-\mu} \mathfrak{Q}_1^{p^{\varkappa-\nu+\mu}} \right) \mathfrak{Q}_1^{\nu p^{\varkappa}(p-1)},$$

also auch

$$p^{i-\nu-1} \mathfrak{Q}_1^{p^{\varkappa}((\nu+1)p-\nu)} \equiv 0 \left(\sum_{\mu=\nu+2}^{i-\varkappa+\nu} p^{i-\mu} \mathfrak{Q}_1^{p^{\varkappa-\nu+\mu}} \right) \mathfrak{Q}_1^{\nu p^{\varkappa}(p-1)}.$$

Daher ist das erste Glied des Ideals rechts in 4) (für $\nu_1 = \nu - 1$)

$$p^{i-\nu-1}\,\mathfrak{Q}_1^{p^{\varkappa-\nu+\mu+1}+(\lambda-\nu)p^{\varkappa+1}(p-1)+(\lambda-1)p^{\varkappa}(p-1)} \equiv 0\left(\sum_{\mu=\nu+2}^{i-\varkappa+\nu-1} p^{i-\mu}\,\mathfrak{Q}_1^{p^{\varkappa-\nu+\mu}}\right)\mathfrak{Q}_1^{\nu p^{\varkappa}(p-1)+\gamma},$$

wobei

$$\begin{aligned}\gamma &= p^{\varkappa+2} + (\nu-\lambda)\,p^{\varkappa+1}(p-1) + (\lambda-1)\,p^{\varkappa}(p-1) - p^{\varkappa+1} - \nu p^{\varkappa}(p-1)\\ &= (\nu+1-\lambda)\,p^{\varkappa+1}(p-1) - (\nu+1-\lambda)\,p^{\varkappa}(p-1)\\ &= (\nu+1-\lambda)p_{\varkappa}\,(p-1)^2 \geqq 0 \quad \text{für} \quad \lambda \leqq \nu+1,\end{aligned}$$

also

$$\nu p^{\varkappa}(p-1) + \gamma = (\nu+1-\lambda)\,p^{\varkappa+1}\,(p-1) + (\lambda-1)\,p^{\varkappa}\,(p-1).$$

Daher ist das erste Glied des Ideals rechts in 4) (für $\nu_1 = \nu - 1$) teilbar durch

$$\left(\sum_{\mu=\nu+2}^{i-\varkappa+\nu} p^{i-\mu}\,\mathfrak{Q}_1^{p^{\varkappa-\nu+\mu}}\right)\mathfrak{Q}_1^{(\nu+1-\lambda)p^{\varkappa+1}(p-1)+(\lambda-1)p^{\varkappa}(p-1)}$$

$$\lambda = 1, 2, \ldots, \nu_1.$$

Die weiteren Glieder des Ideals rechts in 4) sind sämtlich ebenfalls durch dieses Ideal teilbar. Also ergibt 4):

4a) $$p^{i-\lambda}u^{p^{\varkappa}(\lambda p-(\lambda-1))} \equiv 0\left(\sum_{\mu=\nu+2}^{i-\varkappa+\nu} p^{i-\mu}\,\mathfrak{Q}_1^{p^{\varkappa-\nu+\mu}}\right)\mathfrak{Q}_1^{(\nu+1-\lambda)\,p^{\varkappa+1}(p-1)+(\lambda-1)p^{\varkappa}(p-1)},$$

zunächst für $\lambda = 1, 2, \ldots, \nu$, wegen 5) aber auch für $\lambda = \nu + 1$. Damit ist 4) durch vollständige Induktion allgemein bewiesen. Für $\varkappa = \nu$ liefert 4α) die zu beweisenden Formeln (6. 1) (mit λ statt ν). Die Beschränkung auf $\varkappa \leqq i - 1$ ergibt sich daraus, daß in (6. 1) ν die Werte $1, \ldots, \varkappa + 1$ annehmen und der Faktor $p^{i-\nu}$ keinen negativen Exponenten haben darf.

Es ist klar, daß auf Grund von Hilfssatz 3 (bzw. Hilfssatz 2) jede Aussage über die Teilbarkeit des aus allen $u^{p^{\varkappa}(\nu p-\nu+1)}$ in $\mathfrak{Q}$ erzeugten Ideals $\mathfrak{J}_{\varkappa,\nu}$ vermöge des Satzes von den Dimensionsgruppen eine Aussage über Kommutatorbeziehungen in $\mathfrak{G}$ ist. Wenn sich z. B. zeigt, daß eine gewisse Potenz $\mathfrak{Q}^n$ durch das aus allen u^{p^i} erzeugte Ideal $\mathfrak{J}_{i,1}$ teilbar ist, so ist darin die Aussage enthalten, daß $\mathfrak{G}_n/\mathfrak{G}_{n+1}$ höchstens vom Typus $(p^{i-1}, p^{i-1}, p^{i-1}, \ldots, p^{i-1})$ sein kann, usw.; wenn etwa $\mathfrak{Q}^{n_1}$ durch das Ideal aller $u^{ip^i-(i-1)p^{i-1}}$ teilbar ist, so ist sogar $\mathfrak{G}_{n_1} = \mathfrak{G}_{n_1+1}$. Diese Möglichkeiten sollen hier nicht weiter verfolgt werden, wir wollen vielmehr den Hilfssatz 3 in anderer Weise benutzen, um Kommutatorbeziehungen abzuleiten.

Zunächst erhält man genau wie Satz 1:

Satz 1a. *Es ist*

α) $$(t, s, 2p^{\varkappa}(\nu p - \nu + 1) - 1)^{p^{i-\nu}} \equiv 1\ (\mathfrak{U}_{2p^{\varkappa}(\nu p-\nu+1)+1}),$$
$$\varkappa = 0, 1, \ldots, i-2;\ \ \nu = 1, 2, \ldots, \varkappa + 1,$$

β) $$(t, s, 2p^{i-1}(\nu p - \nu + 1) - 1)^{p^{i-\nu}} \equiv 1\ (\mathfrak{U}_{2p^{i-1}(\nu p-\nu+1)+1})$$
$$\nu = 1, 2, \ldots, i.$$

Der Beweis ist derselbe wie zu Satz 1.

Indessen sind damit die Formeln von Hilfssatz 3 nicht voll ausgenutzt. Zunächst sei $S = 1 + u_1 = (1 + u)\ (1 + v)^{\alpha} = 1 + u + \alpha v + \alpha uv + \cdots$; wir ersetzen also in den Formeln (6) u durch $u + \alpha v + \alpha uv + \cdots$. Das ergibt sofort:

(7) $$p^{i-\nu}(u + \alpha v)^{p^{\varkappa}(\nu p-\nu+1)} \equiv 0\ (\mathfrak{Q}_1^{p^{\varkappa}(\nu p-\nu+1)+1}), \qquad \varkappa = 0, 1, \ldots, i-2,$$

und

$$p^{i-\nu}(u + \alpha v)^{p^{i-1}(ip-i+1)} \equiv 0 \ (\mathfrak{Q}^{p^{i-1}(ip-i+1)+1}).$$

Hierbei kann α jede natürliche Zahl sein; wegen $p^i \mathfrak{Q} = 0$ kann mod p^ν reduziert werden. Nehmen wir zunächst $\nu = 1$; bezeichne $\Sigma u^m v^n$ die Summe aller Produkte aus m Faktoren u und n Faktoren v. Dann erhält man:

$$-\sum_{\alpha=1}^{p-1} \alpha^{p-2} p^{i-1}(u + \alpha v)^{p^{\varkappa+1}} \equiv 0 \ (\mathfrak{Q}_1^{p^{\varkappa+1}+1})$$

$$\equiv p^{i-1} \Sigma u^{p^{\varkappa+1}-1} v + p^{i-1} \Sigma u^{p^{\varkappa+1}-p} v^p + p^{i-1} \Sigma u^{p^{\varkappa+1}-2p+1} v^{2p-1} + \cdots.$$

Für $\varkappa = 0$ hat man so

$$p^{i-1} \Sigma u^{p-1} v \equiv 0 \ (\mathfrak{Q}_1^{p+1}). \tag{8}$$

Nun ist mod p^i

$$p^{i-1} \Sigma u^{p-1} v \equiv p^{i-1} \sum_{k=0}^{p-1} (-1)^k \binom{p-1}{k} u^k v u^{p-1-k}$$

$$= p^{i-1}((\ldots((v \circ \underbrace{u) \circ u) \ldots) \circ u}_{p-1}),$$

also:

$$(t, s, p-1)^{p^{i-1}} \equiv 1 \ (\mathfrak{G}_{p+1}). \tag{9}$$

Für $i = 1$ ist das die von *Zassenhaus*[9]) bewiesene Identität. (9) ergibt sofort:

Satz 2.

$$\Pi (t, s_1, s_2, \ldots, s_{p-1})^{p^{i-1}} \equiv 1 \ (\mathfrak{G}_{p+1}), \tag{9a}$$

wobei das Produkt Π *über alle Vertauschungen von* $s_1, s_2, \ldots$ *genommen wird und* $t, s_1, s_2, \ldots, s_{p-1}$ *beliebige ganz oder teilweise gleiche oder verschiedene Elemente aus* $\mathfrak{G}$ *sein können.*

Daraus erhält man wieder:

$$\Pi (t, s_1, s_2, \ldots, s_{p-1}, t_1, t_2, \ldots, t_n)^{p^{i-1}} \equiv 1 \ (\mathfrak{G}_{p+n+1}), \tag{10}$$

wobei das Produkt wieder über die Vertauschungen von $s_1, s_2, \ldots, s_{p-1}$ *erstreckt wird und* n *sowie* $t, t_1, \ldots, t_n, s_1, \ldots, s_{p-1}$ *beliebige Elemente aus* $\mathfrak{G}$ *sind, und ebenso*

$$\Pi (t, t_1, s_1, s_2, \ldots, s_{p-1}, t_2, \ldots, t_n)^{p^{i-1}} \equiv 1 \ (\mathfrak{G}_{p+n+1})$$

$$\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \tag{11}$$

$$\Pi (t, t_1, t_2, \ldots, t_n, s_1, s_2, \ldots, s_{p-1})^{p^{i-1}} \equiv 1 \ (\mathfrak{G}_{p+n+1}).$$

Daraus hat man: In dem Lieschen Ring Λ über dem Ring der mod p ganzen Zahlen sei $\mathfrak{J}$ das aus allen $u \circ v^{p-1}$ erzeugte Ideal und $\Lambda_1 = \Lambda/\mathfrak{J}$. Wenn $\Lambda_1^n = 0$ ist, so ist $\mathfrak{G}_n/\mathfrak{G}_{n+1}$ höchstens vom Typus $(p^{i-1}, p^{i-1}, \ldots, p^{i-1})$.

§ 2.

Es werde zunächst einschränkend vorausgesetzt, daß in $\mathfrak{G}$ in der Untergruppe $\{T, S\} = \mathfrak{U}$ alle Kommutatoren aus $\mathfrak{U}$, die T zweimal als transformierendes Element enthalten, gleich 1 seien; also $(T, S, T) = (T, S, S, T) = \cdots = (T, S; T, S, S) = \cdots = 1$. Dann gilt

Hilfssatz 1. *Es ist für beliebige* n

$$(T, S^n) = \prod_{k=1}^{n} (T, S, k)^{\binom{n}{k}}.$$

---

[9]) Siehe Anm. [4]). Das obige weitergehende Resultat hat der Verfasser unabhängig und vor der Veröffentlichung von Zassenhaus gefunden.

Beweis. Es ist allgemein identisch auch ohne die obige Voraussetzung über T und S:

$$(T, S^n) = (T, S^{n-1})\,(T, S)\,(T, S, S^{n-1}) \text{ für beliebige } n > 0.$$

Daraus erhält man durch wiederholte Anwendung sofort: Der Kommutator (T, S^n) läßt sich als Produkt von Kommutatoren (T, S, k), $k = 1, \ldots, n$, schreiben. Es gilt weiter: In diesem so entwickelten Produkt tritt der Kommutator (T, S, k) abgesehen von der Reihenfolge genau $\binom{n}{k}$-mal als Faktor auf. Denn es ist identisch $(T, S^2) = (T, S)^2 (T, S, S)$; für $n = 2$ tritt also $(T, S, 1)$ genau $\binom{2}{1}$-mal und $(T, S, 2)$ genau $\binom{2}{2}$-mal als Faktor auf; volle Induktion über n ergibt nun zunächst, daß in dem entwickelten Kommutator $(T, S^n) = \Pi(T, S, k)$ der Kommutator (T, S, k) genau $\binom{n}{k}$-mal als Faktor auftritt; und falls, wie vorausgesetzt $((T, S, k), (T, S, l)) = 1$ ist, folgt daraus:

$$(T, S^n) = \prod_{k=1}^{n} (T, S, k)^{\binom{n}{k}}.$$

Hilfssatz 2. *Es ist für beliebige n*

$$(S^{-1}T)^n = \prod_{k=1}^{n} (T, S, k)^{\binom{n+1}{k+1}} T^n S^{-n}.$$

Beweis. $(S^{-1}T)^n = S^{-1}TS^{-1}T \ldots S^{-1}T$

$$= \prod_{r=1}^{n} S^{-r}TS^r \cdot S^{-n}$$

$$= \prod_{r=1}^{n} (T\,(T, S^r)) \cdot S^{-n}$$

$$= \prod_{r=1}^{n} (T, S^r) \cdot T^n S^{-n}$$

$$= \left(\prod_{r=1}^{n} \prod_{k=1}^{r} (T, S, k)^{\binom{r}{k}} \right) T^n S^{-n}$$

$$= \prod_{k=1}^{n} (T, S, k)^{\binom{n+1}{k+1}} T^n S^{-n}$$

w. z. b. w.

Hilfssatz 2 gibt für $n = p^i - 1$, auf $\mathfrak{G}$ angewandt:

$$(S^{-1}T)^{p^i-1} = T^{-1}S = \prod_{k=1}^{p^i-1} (T, S, k)^{\binom{p^i}{p+1}} \cdot T^{-1}S,$$

also

Satz 1.

$$\prod_{k=1}^{p^i-1} (T, S, pk-1)^{\binom{p^i}{pk}} = 1.$$

Schreiben wir diese Formel additiv, wobei $(T, S, k-1)$ durch u^k vertreten werde, so ist also

$$\sum_{k=1}^{p^i-1} \binom{p^i}{pk} u^{pk} = 0. \tag{1}$$

Ersetzt man T durch (T, S), so gilt der Satz wiederum, es ist also

$$\prod_{k=1}^{p^i-1} (T, S, pk)^{\binom{p^i}{pk}} = 1$$

und demnach auch

$$\sum_{k=1}^{p^{i-1}} \binom{p^i}{pk} u^{pk+1} = 0, \tag{2}$$

usw., d. h. Formel (1) bleibt richtig, wenn man mit irgendeiner Potenz von u multipliziert. Weiterhin gilt auch $p^i u = 0$ usw., da ja $(T, S)^{p^i} = 1$ usw. Es gelten also für die Behandlung von Formel (1) genau die gleichen Gesetze, die für die formal gleichen Formeln in § 1 galten, und wir können daher die dort in Hilfssatz 3 gewonnenen Resultate sofort hierher übertragen; unter den dort als Kongruenzmoduln auftretenden Potenzen des Teilringes $\{u\} = \mathfrak{L}_1$ haben wir hier zu verstehen:

$\mathfrak{L}_1^n$ ist die kleinste Untergruppe $\mathfrak{U}_n$, die alle $(T, S, n-1)$ enthält, $n = 2, 3, \ldots$; $\mathfrak{L}_1$ selbst (das allerdings nicht auftritt) wäre $\{T\}$. Unter $p^q L_1^n$ ist die kleinste Untergruppe zu verstehen, die alle p^q-ten Potenzen von Elementen aus $\mathfrak{U}_n$ enthält; solche Gruppen mögen hier $(\mathfrak{U}_n)^{p^q}$ genannt werden; das in § 1 (6) auftretende Ideal in $\mathfrak{L}_1$:

$$\left(\sum_{\mu=\varkappa+2}^{i} p^{i-\mu}\, \mathfrak{L}_1^{p^\mu}\right) \mathfrak{L}_1^{(\varkappa+1-\nu)p^{\varkappa+1}(p-1)+(\nu-1)p^\varkappa(p-1)}$$

ist nunmehr die Vereinigungsgruppe

$$\prod_{\mu=\varkappa+2}^{i} (\mathfrak{U}_{p^\mu+(\varkappa+1-\nu)p^{\varkappa+1}(p-1)+(\nu-1)p^\varkappa(p-1)})^{p^{i-\mu}},$$

usw. Kehren wir nunmehr zu der multiplikativen Schreibweise zurück, so ergeben die Gleichungen § 1 (6):

$$\text{A)}\quad (T, S, p^\varkappa(\nu p - \nu + 1) - 1)^{p^{i-\nu}} \equiv 1 \left(\prod_{\mu=\varkappa+2}^{i} (\mathfrak{U}_{p^\mu+(\varkappa+1-\nu)p^{\varkappa+1}(p-1)+(\nu-1)p^\varkappa(p-1)})^{p^{i-\mu}}\right),$$

$$\varkappa = 0, 1, \ldots, i-2;\ \nu = 1, 2, \ldots, \varkappa+1, \tag{3}$$

$$\text{B)}\qquad (T, S, \nu p^i - (\nu-1)\, p^{i-1} - 1)^{p^{i-\nu}} = 1, \qquad \nu = 1, 2, \ldots, i.$$

Wir haben hierbei $(T, S, T) = (T, S, ST) = (T, S; T, S, S) = \cdots = 1$ gesetzt. Wählt man T aus $\mathfrak{G}_n$, n beliebig, so liegen alle diese gleich 1 gesetzten Elemente in $\mathfrak{G}_{2n+1}$, und man hat auf der rechten Seite nur $\mathfrak{G}_{2n+1}$ hinzuzufügen, um ohne Einschränkung geltende Gleichungen zu erhalten; bezeichnen wir, um die langen Indizes zu entfernen, für jedes Zahlentripel $\mu, \nu, \varkappa$ die Zahl $p^\mu + (\varkappa+1-\nu)p^{\varkappa+1}(p-1) + (\nu-1)p^\varkappa(p-1)$ mit $n(\mu, \nu, \varkappa)$, so liegt für $T \in \mathfrak{G}_n$ die Gruppe $\mathfrak{U}_{n(\mu,\nu,\varkappa)}$ in $\mathfrak{G}_{n+n(\mu,\nu,\varkappa)-1}$. Daher hat man nun ohne Einschränkung mit $T_n \in \mathfrak{G}_n$:

Satz 2. A) $$(T_n, S, p^\varkappa(\nu p - \nu + 1) - 1)^{p^{i-\nu}} \equiv 1 \left(\prod_{\mu=\varkappa+2}^{i} (\mathfrak{G}_{n+n(\mu,\nu,\varkappa)})^{p^{i-\mu}}\, \mathfrak{G}_{2n+1}\right),$$

$$\varkappa = 0, 1, \ldots, i-2;\ \nu = 1, 2, \ldots, \varkappa+1, \tag{4}$$

$$\text{B)}\quad (T_n, S, \nu p^i - (\nu-1)\, p^{i-1} - 1)^{p^{i-\nu}} \equiv 1\ (\mathfrak{G}_{2n+1}), \qquad \nu = 1, 2, \ldots, i.$$

Z. B. gibt (4. A) für $\varkappa = 0$, $\nu = 1$ und

$$\begin{aligned} &n = p: && (T_p, S, p-1)^{p^{i-1}} \equiv 1\ (\mathfrak{G}_{2p+1}),\\ &n = p+1: && (T_{p+1}, S, p-1)^{p^{i-1}} \equiv 1\ (\mathfrak{G}_{2p+3}),\\ &n = p+2: && (T_{p+2}, S, p-1)^{p^{i-1}} \equiv 1\ (\mathfrak{G}_{2p+5}), \end{aligned} \tag{5}$$

usw. Durch geeignete Wahl von n kann man stets erreichen, daß in den Gleichungen (4. A) und (4. B) die Kommutatoren auf der linken Seite formal etwa in $\mathfrak{G}_m$ liegen, während die rechte Seite in $\mathfrak{G}_{m+q}$ liegt, $q > 0$ beliebig. Dies ergibt Möglichkeiten, Formeln zu entwickeln, die viel weiter gehen, als die aus § 1, Satz 1 und Satz 1a folgenden Formeln.

Denn die dort gefundenen Formeln sind von der Form $(T, S, n) \equiv 1\ (\mathfrak{G}_{n+2})$; sie geben also bei der Substitution $S = \Pi S_k^{\alpha_k}$ immer nur Formeln für Ausdrücke von der Form

$$\Pi(T, \underbrace{S_1, S_1, \ldots, S_1}_{r_1}, \underbrace{S_2, S_2, \ldots, S_2}_{r_2}, \ldots),$$

wobei das Produkt über alle Anordnungen von r_1 Elementen S_1, r_2 Elementen $S_2, \ldots$ zu erstrecken ist; diese Formeln sind also gewissermaßen symmetrisch. Hier dagegen können wir von vornherein unsymmetrische Formeln bilden, die also bessere Aussicht bieten, durch weitere Kommutatorbildung usw. schließlich alle Elemente einer Untergruppe $\mathfrak{G}_s$ der absteigenden Zentrenreihe durch p^i-te Potenzen und Elemente aus $\mathfrak{G}_{s+1}$ auszudrücken. Wir wollen allgemein zeigen, wie man aus den Formeln (4. A), (4. B) unsymmetrische Formeln gewinnt. Es gelte wie oben, daß jeder Kommutator, in dem T mindestens zweimal als transformierendes Element auftritt, gleich 1 sei. Setzt man

$$(T, S, k) = (T, S_1 S_2 \cdots S_r, k) = \Pi(T, S_{i_1}, S_{i_2}, \ldots, S_{i_q})^{\alpha^{(k)}_{i_1, i_2, \ldots, i_q}},$$

wobei das Produkt Π die volle Entwicklung von (T, S, k) für $S = S_1 S_2 \cdots S_r$ sei, so ist $\alpha^{(k)}_{i_1, i_2, \ldots, i_q}$ gleich dem Koeffizienten von $S_{i_1} S_{i_2} \cdots S_{i_q}$ in der Entwicklung von $((1 + S_1)(1 + S_2) \cdots (1 + S_r) - 1)^k$.

Für $k = 1$ und $r = 2$ bestätigt man nämlich (unter Berücksichtigung von $((T, S_1), (T, S_2)) = 1$ direkt:

$$(T, S_1 S_2) = (T, S_1)(T, S_2)(T, S_1, S_2).$$

Vollständige Induktion zuerst für r, dann für k ergibt die Behauptung.

Ferner wird

$$(T, S_1 S_2 \cdots S_r, k)^m = \left(\Pi(T, S_{i_1}, S_{i_2}, \ldots, S_{i_q})^{\alpha^{(k)}_{i_1, i_2, \ldots, i_q}}\right)^m$$

$$= \Pi(T, S_{i_1}, S_{i_2}, \ldots, S_{i_q})^{m\, \alpha^{(k)}_{i_1, i_2, \ldots, i_q}},\ m \text{ beliebig.}$$

Unsere Annahme, daß $(T, S, T), \ldots = 1$ seien, ist nun im Sinne der Kongruenz (4) erfüllt. Setzt man also z. B. in der ersten Gleichung (5) $S = S_1 S_2 \cdots S_p$, so hat man in $\left(\prod_{i=1}^{p}(1 + S_i) - 1\right)^{p-1}$ die Koeffizienten derjenigen Produkte zu berechnen, die sich aus $p - 1$ oder aus p Faktoren zusammensetzen, denn die Kommutatoren, die den aus mehr als p Faktoren zusammengesetzten Produkten entsprechen, liegen von vornherein in $\mathfrak{G}_{2p+1}$. So erhält man eine Formel:

$$(6)\quad \Pi(T_p, S_{i_1}, \ldots, S_{i_{p-1}})^{p^{i-1}\alpha_{i_1, i_2, \ldots, i_{p-1}}}\, \Pi(T_p, S_{i_1}, \ldots, S_{i_p})^{p^{i-1}\alpha_{i_1, \ldots, i_p}} \equiv 1\ (\mathfrak{G}_{2p+1}).$$

Nun sei p ungerade. Ersetzt man in (6) unabhängig voneinander alle S_i durch S_i^{α}, potenziert jedesmal die Formel mit α^{p-2} und bildet das Produkt aller sich so ergebenden Formeln für $\alpha = 1, 2, \ldots, p - 1$, so treten in dem endgültigen Produkt alle Kommutatoren, in denen nicht alle Indizes $i_1, i_2, \ldots, i_p$ verschieden sind, mit dem Exponenten p^i auf, werden also gleich 1. Es folgt dann:

$$(7)\qquad \Pi(T_p, S_{i_1}, S_{i_2}, \ldots, S_{i_p})^{p^{i-1}\alpha_{i_1, i_2, \ldots, i_p}} \equiv 1\ (\mathfrak{G}_{2p+1}),$$

wobei $i_1, i_2, \ldots, i_p$ sämtlich verschieden sind. Wir haben also die $\alpha_{i_1, i_2, \ldots, i_p}$ für jede Reihenfolge verschiedener $i_1, i_2, \ldots, i_p$ in $\left(\prod_{i=1}^{p}(1 + S_i) - 1\right)^{p-1}$ zu bestimmen. Setzt man

$\sum_{i=1}^{p} S_i = \sigma_1$ und $\sum_{i<k}^{1,p} S_i S_k = \sigma_2$, so ergibt sich sofort, daß man nur den Koeffizienten von $S_{i_1} S_{i_2} \cdots S_{i_p}$ in $\sigma_1^{p-2}\sigma_2 + \sigma_1^{p-3}\sigma_2\sigma_1 + \cdots + \sigma_2\sigma_1^{p-2}$ zu bestimmen hat. Dieser Koeffizient ist gleich der Anzahl derjenigen Indexpaare i_q, i_{q+1} in $i_1, i_2, \ldots, i_p$, für die $i_q < i_{q+1}$ ist.

Sei nämlich $S_{i_1} S_{i_2} \cdots S_{i_p}$ auf alle Arten zerlegt in

$$(S_{i_1} S_{i_2} \cdots S_{i_{r-1}}) \cdot (S_{i_r} S_{i_{r+1}}) \cdot (S_{i_{r+2}} \cdots S_{i_p}).$$

Das Produkt $S_{i_1} S_{i_2} \cdots S_{i_{r-1}}$ kommt in σ_1^{r-1} genau einmal vor, das Produkt $S_{i_r} S_{i_{r+1}}$ kommt in σ_2 genau einmal oder gar nicht vor, je nachdem $i_r < i_{r+1}$ ist oder nicht; das Produkt $S_{i_{r+2}} \cdots S_{i_p}$ kommt in σ_1^{p-r-1} genau einmal vor; also kommt das Produkt $S_{i_1} S_{i_2} \cdots S_{i_p}$ in einem Summanden $\sigma_1^{r-1}\sigma_2\sigma_1^{p-r-1}$ genau einmal oder gar nicht vor, je nachdem $i_r < i_{r+1}$ ist oder nicht. Daraus folgt die Behauptung.

Definieren wir nun: $(T, S_{i_1}, S_{i_2}, \ldots, S_{i_p})$ geht aus $(T, S_1, S_2, \ldots, S_p)$ hervor durch symbolische Potenzierung mit dem Permutationsoperator[10]) $P = \begin{pmatrix} 1, & 2, & \ldots, & p \\ i_1, & i_2, & \ldots, & i_p \end{pmatrix}$, so können wir (7) in der einfacheren Form

$$(T_p, S_1, S_2, \ldots, S_p)^{p^{i-1} \sum_P \alpha^P P} \equiv 1 \ (\mathfrak{G}_{2p+1}) \tag{8}$$

schreiben. Hierbei ist α^P gleich der Anzahl von Paaren aufeinander folgender Indizes i_r, i_{r+1} mit $i_r < i_{r+1}$ in der unteren Zeile der Permutation $P = \begin{pmatrix} 1, & 2, & \ldots, & p \\ i_1, & i_2, & \ldots, & i_p \end{pmatrix}$, und die $\sum_P$ wird erstreckt über alle Permutationen der symmetrischen Gruppe $\mathfrak{S}_p$. Da nun $S_1, S_2, \ldots, S_p$ ganz beliebig gewählt werden können, gilt (8) auch für jede durch Ausübung eines Operators $P_1 = \begin{pmatrix} 1, & 2, & \ldots, & p \\ r_1, & r_2, & \ldots, & r_p \end{pmatrix}$ daraus hervorgehende Form. Es ist also

$$(T_p, S_1, S_2, \ldots, S_p)^{p^{i-1} (\sum_P \alpha^P P) P_1} \equiv 1 \ (\mathfrak{G}_{2p+1}), \quad P_1 \in \mathfrak{S}_p. \tag{9}$$

Läßt man in (9) P_1 alle Elemente aus $\mathfrak{S}_p$ durchlaufen, so erhält man ein Gleichungssystem für alle $(T_p, S_{i_1}, S_{i_2}, \ldots, S_{i_p})^{p^{i-1}}$, dessen Determinante gleich der Determinante der Matrix $\sum_P \alpha^P \overline{P}$ ist, wobei $\overline{P}$ die Matrix von P in der regulären Darstellung von $\mathfrak{S}_p$ ist. Die Determinante $\left| \sum_P \alpha^P \overline{P} \right|$ wird allerdings $\equiv 0 \bmod p$; aber man hat noch zwei weitere Gleichungssysteme zur Verfügung. Seien nämlich $\mathfrak{U}_1$ bzw. $\mathfrak{U}_2$ diejenigen Untergruppen von $\mathfrak{S}_p$, welche die Ziffern 1 bzw. p, d. h. hier S_1 bzw. S_p invariant lassen, so hat man noch:

$$(T_p, S_1, \ldots, S_p)^{p^{i-1} (\sum_{U \in \mathfrak{U}_1} U) P} \equiv 1 \ (\mathfrak{G}_{2p+1}), \quad P \in \mathfrak{S}_p \tag{10a}$$

und

$$(T_p, S_1, \ldots, S_p)^{p^{i-1} (\sum_{U \in \mathfrak{U}_2} U) P} \equiv 1 \ (\mathfrak{G}_{2p+1}), \quad P \in \mathfrak{S}_p. \tag{10b}$$

Für $p = 3$ reichen diese Systeme aus, um $(T_3, S_1, S_2, S_3)^{3^{i-1}}$ zu bestimmen, wie nachher gezeigt werden wird. Nun kann T_3 jedes Element aus $\mathfrak{G}_3$, S_1, S_2, S_3 jedes System von drei verschiedenen oder gleichen Elementen aus $\mathfrak{G}$ sein; mithin kann (T_3, S_1, S_2, S_3) jedes Element aus $\mathfrak{G}_6$ sein, und wir haben:

---

[10]) Solche Permutationsoperatoren hat auch Witt mehrfach angewandt.

Ist $\mathfrak{G}(3^i) = 1$, so ist $\mathfrak{G}_n/\mathfrak{G}_{n+1}$ höchstens vom Typus $(3^{i-1}, 3^{i-1}, \ldots, 3^{i-1})$, $n \geqq 6$. Dies gilt unabhängig davon, wie viele Elemente $\mathfrak{G}$ erzeugen.

Für $p = 2$ hat man natürlich ohne weitere Rechnung: Ist $\mathfrak{G}(2^i) = 1$, so ist $\mathfrak{G}_n/\mathfrak{G}_{n+1}$ höchstens vom Typus $(2^{i-1}, 2^{i-1}, \ldots, 2^{i-1})$, $n \geqq 2$.

Die Rechnung, die wir hier für $(T_p, S, p-1)^{p^{i-1}}$ durchgeführt haben, können wir ohne weiteres auf den allgemeinen Fall

$$(T_q, S, q-1)^{p^{i-\nu}} \equiv 1 \ (\mathfrak{G}_{2q+1})$$

übertragen, wobei zur Abkürzung $p^\varkappa(\nu p + \nu - 1) = q$ gesetzt ist, $\nu = 1, 2, \ldots, \varkappa + 1$, $\varkappa = 0, 1, \ldots, i-1$. Man hat nur S durch $S_1 S_2 \cdots S_q$ und (siehe den Text nach (6)) alle S_i unabhängig voneinander durch $S_i^{\alpha p^{\nu-1}}$ zu ersetzen, mit $\alpha^{(p-2)p^{\nu-1}}$ zu potenzieren und das Produkt über $\alpha = 1, 2, \ldots, p-1$ zu bilden. Man erhält die folgende Verallgemeinerung von (8):

$$(11) \qquad (T_q, S_1, S_2, \ldots, S_q)^{p^{i-\nu} \sum_{P \in \mathfrak{S}_q} \alpha^P P} \equiv 1 \ (\mathfrak{G}_{2q+1}).$$

Selbstverständlich sind die Formeln (8) und (11) nur als einfachste Beispiele dafür gedacht, wie man aus den Grundbeziehungen (4) weitere Beziehungen ableitet. Wir wollen uns aber auf diese beschränken, da es doch unmöglich scheint, auch nur eine allgemeine Übersicht über die erhaltbaren Formeln zu geben. Man bedenke, daß z. B. aus

$$(T_q, S_1, S_2, \ldots, S_q)^{p^{i-\nu} \sum_{P \in \mathfrak{S}_q} \alpha^P P} \equiv 1 \ (\mathfrak{G}_{2q+1})$$

folgt

$$(T_q, S_1, S_2, \ldots, S_q, R_1, R_2, \ldots, R_l)^{p^{i-\nu} \sum_{P \in \mathfrak{S}_q} \alpha^P P} \equiv 1 \ (\mathfrak{G}_{2q+l+1})$$

und

$$(T_q, R_1, S_1, S_2, \ldots, S_q, R_2, \ldots, R_l)^{p^{i-\nu} \sum_{P \in \mathfrak{S}_q} \alpha^P P} \equiv 1 \ (\mathfrak{G}_{2q+l+1})$$
$$\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots$$

und daß dies wieder für alle Vertauschungen von $R_1, R_2, \ldots, R_l$ gilt, weiter daß man in $(T, S, q-1)^{p^{i-\nu}}$ ja auch S durch $S_1 S_2 \cdots S_{q+1}$ oder $S_1 S_2 \cdots S_{q+2}$ usw. ersetzen kann, und daß man eine ähnliche Rechnung wie die obige durchführen kann, wenn man T durch $T_{q+1} \in \mathfrak{G}_{q+2}$ bzw. $T_{q+2} \in \mathfrak{G}_{q+2}$ usw. ersetzt. Speziell im Falle $q+1$ tritt ein symbolischer Exponent $\Sigma \beta^P P$ auf, wobei β^P für jede Permutation $P = \begin{pmatrix} 1, & 2, & \ldots, & q+1 \\ i_1, & i_2, & \ldots, & i_{q+1} \end{pmatrix}$ die Anzahl der Tripel in der unteren Reihe mit $i_r < i_{r+2} < i_{r+1}$ ist. Andererseits gelten für $(T_{q+1}, S_1, S_2, \ldots, S_{q+1})$ ja auch die Formeln (11) mit $T_q = (T_{q+1}, S_1)$ und $S_2, S_3, \ldots, S_{q+1}$ für $S_1, S_2, \ldots, S_q$, sowie mit T_{q+1} für T_q und

$$(T_{q+1}, S_1, S_2, \ldots, S_{q+1}) = ((T_{q+1}, S_1, S_2, \ldots, S_q), S_{q+1}),$$

angewandt auf $S_1, S_2, \ldots, S_q$, usw. Kurz, es entsteht eine Fülle von Beziehungen, in die ich noch keine vollständige Übersicht bringen konnte. Ich muß mich daher mit den vorstehenden Andeutungen begnügen, möchte aber im folgenden Paragraphen noch auf einen für die weitere Bearbeitung in Frage kommenden Gesichtspunkt hinweisen.

§ 3.

Sei $\mathfrak{G}(3^i) = 1$; wählt man $T \in \mathfrak{G}_3$, so ist nach § 2, (4. A)

$$(T, S, S)^{3^{i-1}} \equiv 1 \ (\mathfrak{G}_7).$$

Setzt man $S = S_1 S_2 S_3$, so findet man leicht:

$$(T, S_1, S_2, S_3)^{3^{i-1} \Sigma \alpha^P P} \equiv 1 \ (\mathfrak{G}_7),$$

wobei die P Permutationsoperatoren sind, die in (T, S_1, S_2, S_3) eine Permutation der Elemente S_1, S_2, S_3 bewirken und Σ über alle Permutationen aus der symmetrischen Gruppe $\mathfrak{S}_3$ erstreckt wird. α^P ist zu jeder Permutation P wieder die Zahl, die angibt, wie viele Indexpaare $i_r < i_{r+1}$ in $P = \begin{pmatrix} 1 & 2 & 3 \\ i_1 & i_2 & i_3 \end{pmatrix} = \begin{pmatrix} S_1 & S_2 & S_3 \\ S_{i_1} & S_{i_2} & S_{i_3} \end{pmatrix}$ auftreten. Geht man zur additiven Schreibweise über, so hat man

$$3^{i-1} t u_1 u_2 u_3 \Sigma \alpha^P P = 0. \tag{1}$$

Seien

$$P_1 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \ P_2 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \ P_3 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}, \ P_4 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}, \ P_5 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}, \ P_6 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix},$$

so wird $\alpha^{P_1} = 2$, $\alpha^{P_2} = \alpha^{P_3} = \alpha^{P_4} = \alpha^{P_5} = 1$, $\alpha^{P_6} = 0$.

$\Sigma \alpha^P P$ annulliert also $3^{i-1} t u_1 u_2 u_3$, und daher bewirkt auch $\Sigma \alpha^P P \cdot P_i$, $P_i \in \mathfrak{S}_3$ dasselbe.

Wir haben als Folge von $(T, S, S)^{3^{i-1}} \equiv 1 \ (\mathfrak{G}_7)$ aber noch die weiteren Formeln

$$(T, S_1, S_2, R)^{3^{i-1}} (T, S_2, S_1, R)^{3^{i-1}} \equiv 1 \ (\mathfrak{G}_7), \quad R \text{ beliebig}$$

und

$$(T, R, S_2, S_3)^{3^{i-1}} (T, R, S_3, S_2)^{3^{i-1}} \equiv 1 \ (\mathfrak{G}_7), \quad R \text{ beliebig}.$$

Wenn wir in der ersten Formel $R = S_3$, in der zweiten $R = S_1$ setzen und wieder zur additiven Schreibweise übergehen, so gibt das:

$$3^{i-1} t u_1 u_2 u_3 (1 + P_4) P_k = 0, \qquad k = 1, 2, \ldots, 6, \tag{2}$$

$$3^{i-1} t u_1 u_2 u_3 (1 + P_5) P_k = 0, \qquad k = 1, 2, \ldots, 6. \tag{3}$$

Ferner ist natürlich $3^{i-1} t u_1 u_2 u_3 \cdot 3 P_k = 0$, $k = 1, 2, \ldots, 6$.

Wir haben es nunmehr nur mit der Algebra der P zu tun und können den Darstellungsmodul fortlassen.

(1), (2), (3) ergeben

$$\begin{aligned} 2P_1 + P_2 + P_3 + P_4 + P_5 &= 0 \\ P_1 \qquad\quad + P_4 \qquad\quad &= 0 \\ P_1 \qquad\qquad\quad + P_5 &= 0, \end{aligned}$$

daher

$$P_2 + P_3 = 0 = (P_1 + P_2) P_2,$$

also

$$P_1 + P_2 = 0$$

$$P_1 + P_2 - (P_2 + P_3) = 0 = P_1 - P_3.$$

Es ist aber $P_2 P_3 = 1$, so daß auch

$$P_2 P_3 - P_3 = P_2 P_3 - 1 - (P_3 - 1) = 0 = (P_2 - P_1) P_3,$$

$$\text{daher} \qquad P_2 - P_1 = 0 \quad \text{und wegen} \quad P_1 + P_2 = 0$$
$$2P_1 = 0, \quad \text{also wegen} \quad 3^i P_1 = 0$$
$$P_1 = 0, \quad P_1 P_k = P_k = 0$$

folgt, d. h.:

Es ist jedes Element $(T, S_1, S_2, S_3)^{3^{i-1}} \equiv 1\ (\mathfrak{G}_7)$, wenn $T \in \mathfrak{G}_3$ ist; da S_1, S_2, S_3 auch sämtlich oder teilweise gleich sein können, heißt das: $\mathfrak{G}_6/\mathfrak{G}_7$ ist höchstens vom Typus $(3^{i-1}, 3^{i-1}, \ldots, 3^{i-1})$.

Wie man sieht, spielen bei der Rechnung überhaupt nur die Eigenschaften der Operationssymbole eine Rolle, also in diesem speziellen Falle die Eigenschaften der aus den Elementen der symmetrischen Gruppe $\mathfrak{S}_3$ im Primkörper $K(3)$ entstehenden Algebra. Diese weitere Behandlung der hier gefundenen Resultate scheint mir recht aussichtsreich, da sie sich noch erheblich verallgemeinern läßt.

§ 4.

Es seien, nur als einfachste Beispiele, einige Anwendungen der gefundenen Resultate gegeben.

Wird eine Gruppe $\mathfrak{G}$ mit der Bedingung $\mathfrak{G}(p) = 1$ aus r Elementen $t_1, t_2, \ldots, t_r$ erzeugt, so erhält man aus $(a, b, p-1) \equiv 1\ (\mathfrak{G}_{p+1})$, indem man $a = \prod_{i=1}^{r} t_i^{\alpha_i}$, $b = \prod_{i=1}^{r} t_i^{\beta_i}$ setzt, genau $\binom{p+r-3}{r-1}$ unabhängige Elemente; ferner ist nach der Wittschen Formel[1]) der Rang von $\mathfrak{F}_p/\mathfrak{F}_{p+1}$, wenn $\mathfrak{F}$ die aus r freien Elementen erzeugte Gruppe ist, gleich $\frac{r^p - r}{p}$. Daraus folgt leicht, daß $\mathfrak{G}_p/\mathfrak{G}_{p+1}$ höchstens den Rang $\frac{r^p - r}{p} - \binom{p+r-3}{r-1}$ haben kann. Sei $r = 2$, $\mathfrak{G}$ die aus 2 Elementen mit der Bedingung $\mathfrak{G}(5) = 1$ erzeugte Gruppe, $\mathfrak{F}$ die aus 2 freien Erzeugenden entstehende Gruppe. Nach Witt hat

$\mathfrak{F}_5/\mathfrak{F}_6$ den Rang 6,
$\mathfrak{F}_6/\mathfrak{F}_7$ den Rang 9.
$\mathfrak{F}_7/\mathfrak{F}_8$ den Rang 18.

Für $\mathfrak{G}_5/\mathfrak{G}_6$ finden wir nach obiger Überlegung den Rang $6 - 4 = 2$. Aus $(a, b, b, b, b, c) \equiv 1(\mathfrak{G}_7)$ und $(a, c, b, b, b, b) \equiv 1(\mathfrak{G}_7)$ findet man 8 unabhängige Elemente, und eine einfache Überlegung zeigt, daß also $\mathfrak{G}_6/\mathfrak{G}_7$ den Rang $9 - 8 = 1$ hat. Geht man nun zu $\mathfrak{G}_7$ über, so hat man $(a, b, b, b, b, c, d) \equiv 1(\mathfrak{G}_8)$, $(a, c, b, b, b, b, d) \equiv 1(\mathfrak{G}_8)$, $(a, c, d, b, b, b, b) \equiv 1\ (\mathfrak{G}_8)$, $((a, c), (d, b, b, b, b,)) \equiv 1\ (\mathfrak{G}^8)$ und die daraus hervorgehenden Formeln. So erhält man 18 unabhängige Elemente und den Rang von $\mathfrak{G}_7/\mathfrak{G}_8$ mit $18 - 18 = 0$, d. h. $\mathfrak{G}_7 = \mathfrak{G}_8$. Also gilt in jeder endlichen aus 2 Elementen mit der Bedingung $\mathfrak{G}(5) = 1$ erzeugten Gruppe $\mathfrak{G}$, daß $\mathfrak{G}_7 = 1$ ist.

Eine andere Anwendung der gleichen Formel ergibt: Ist p eine Primzahl und $\mathfrak{G}$ eine endliche aus beliebig vielen Elementen mit der Bedingung $\mathfrak{G}(p) = 1$ erzeugte Gruppe, so ist $\mathfrak{G}_{p+1} < \mathfrak{G}^2$, d. h. die $(p+1)$-te Untergruppe der absteigenden Zentrenreihe ist in der zweiten Ableitung von $\mathfrak{G}$ enthalten.

Beweis. Man kann bekanntlich für jedes n eine Basis von $\mathfrak{G}_n/\mathfrak{G}_{n+1}$ in Kommutatoren von der Form $(t_1\ t_2, \ldots, t_n)$ bestimmen. Es genügt also, nachzuweisen, daß jedes Element $(t_1, t_2, \ldots, t_{p+1})$ aus $\mathfrak{G}$ in $\mathfrak{G}^2$ liegt. Nun haben wir gefunden:

(1) $$\Pi(t_1, \underbrace{t_2, t_3, \ldots, t_p}) \equiv 1\ (\mathfrak{G}_{p+1}),$$

wobei das Produkt Π über alle Permutationen der Elemente $t_2, t_3, \ldots, t_p$ erstreckt wird. Nun ist für beliebige $n > 3$:

$$(t_1, t_2, \ldots, t_{n-1}, t_n) \equiv (t_1, t_2, \ldots, t_n, t_{n-1}) \ (\mathfrak{G}^2\mathfrak{G}_{n+1}).$$

Setzt man in (1) $t_1 = (t_1', t_1'')$, so folgt sofort:

$$(t_1', t_1'', t_2, t_3, \ldots, t_p)^{(p-1)!} \equiv 1 \ (\mathfrak{G}^2\,\mathfrak{G}_{p+2}),$$

und, da $t_1', t_1'', t_2, \ldots, t_p$ beliebig gewählt werden können,

$$\mathfrak{G}_{p+1} < \mathfrak{G}^2, \quad \text{w. z. b. w.}$$

Ebenso ergibt § 1, Satz 2 leicht:

Ist $\mathfrak{G}(p^i) = 1$, *so ist* $\mathfrak{G}_{p+1}\,\mathfrak{G}^2/\mathfrak{G}_2$ *höchstens vom Typus* $(p^{i-1}, p^{i-1}, \ldots, p^{i-1})$.

Weitere Anwendungen mögen dem Leser überlassen bleiben; sie dürften noch viele interessante Resultate für p-Gruppen bringen.

Eingegangen 21. August 1939.

Gruppen aus der Klassenkörpertheorie.

Von *Andreas Speiser* in Zürich.

Es sollen einige gruppentheoretische Probleme, welche in der Lehre von den relativ-abelschen Körpern auftreten, behandelt werden.

1. *Die kristallographischen Gruppen.* Wir bezeichnen damit diejenigen Substitutionsgruppen, welche in halbreduzierter Form der Gestalt

$$\begin{pmatrix} E & 0 \\ a & A \end{pmatrix}$$

auftreten, wo E eine Einheitsmatrix, A eine Darstellung der Gruppe ohne die identische Darstellung und a eine rechteckige Matrix bedeuten. Diese Darstellungen spielen eine Rolle bei folgenden Problemen:

a) Es sei K ein relativ-galoisscher Körper über k. Die Grundeinheiten von K erfahren bei der Relativgruppe in den Exponenten eine Substitution der angegebenen Art. Hier läßt sich im allgemeinen a nicht wegschaffen durch Änderung der Basis. Man kommt nun im relativ-zyklischen Fall zur Aufstellung der relativen Grundeinheiten und zur Konstruktion von Einheiten, deren Relativnorm 1 ist und die doch nicht $(1 - S)$-te Potenzen einer Einheit sind.

b) K und k seien absolut galoissch und die Gruppe von K/k sei abelsch vom Typus $P = (p, p, \ldots)$. K sei unverzweigt über k, also ein gewisser Teilkörper des p-Klassenkörpers von k und die Primzahl p gehe in dem Grad von k nicht auf. Es fragt sich, welches Stück dieses Klassenkörpers K man schon an Unterkörper von k anheften kann. Unter den Substitutionen von k erfährt der Normalteiler P einen Automorphismus; wir betrachten davon bloß die Untergruppe, welche zu dem zu untersuchenden Unterkörper gehört. Diese induziert für die Basiselemente von P in den Exponenten eine Substitutionsgruppe, aber diesmal modulo p. Weil p prim ist zur Ordnung der Gruppe, so läßt sich der rechteckige Teil a wegschaffen. Es ergibt sich, daß P zerfällt in das Zentrum (entsprechend E) und einen dazu fremden Normalteiler (entsprechend A). Nun kann man den Satz von Burnside über die Sylowgruppen, die im Zentrum ihres Normalisators liegen, auf die Faktorgruppe dieses Normalteilers anwenden und findet, daß man genau denjenigen Teil des Klassenkörpers, der zum Zentrum gehört, an den Unterkörper anheften kann. Dies läßt sich auf beliebige relativ-abelsche Körper ausdehnen.

2. *Darstellungen.* Mit der Lehre vom Klassenkörper hängt nach den Untersuchungen von Herrn Hasse u. a. aufs engste ein Hauptsatz über die einfachen Algebren zusammen. Man wird hier auf die verschränkten Darstellungen einer Gruppe geführt, wobei Faktoren auftreten. Indem man durch Erweiterung des Körpers die Matrizen so normiert, daß ihre Determinante 1 wird, erreicht man, daß die Faktoren nur noch n-te Einheitswurzeln sein können, wobei n den Grad der Algebra bedeutet. Adjungiert man nun die n-ten

Einheitswurzeln, so liefert die Darstellung mit Faktoren eine solche ohne Faktoren für eine Gruppe, welche die vorige als Faktorgruppe eines Zentrums von der Ordnung n enthält. Läßt sich also der Körper zentral in der angegebenen Weise erweitern, so kann man die Darstellung der Gruppe auf die Identität zurückführen, und es ist dann möglich, die einfache Algebra durch bloße Adjunktion von n-ten Einheitswurzeln auf eine vollständige Matrixalgebra zu reduzieren. In andern Fällen, z. B. wenn die Gruppe zyklisch ist, kommt man durch Adjunktion von n^2-ten Einheitswurzeln zum Ziel. Dies geschieht z. B. bei der Quaternionengruppe, wo man die vierte Einheitswurzel i wirklich braucht, obgleich das Charakterensystem rational ist.

3. *Die Struktur der Zerlegungsgruppe.* Eine rein arithmetische Theorie des Klassenkörpers ist trotz tiefer neuerer Untersuchungen noch nicht gefunden worden. Schon für relativ-zyklische Körper vom Primzahlgrad l läßt sich arithmetisch zwar zeigen, daß die Relativnormen der Klassen des Oberkörpers im Unterkörper in eine Klassengruppe fallen, deren Index mindestens l ist. Daß dagegen dieser Index höchstens l ist, also $= l$, zeigt man mit transzendenten Mitteln. In gewissen Fällen kann man jedoch mit den Formeln auskommen, welche die Struktur der Trägheitsgruppe wiedergeben. Man findet, daß durch die Hilbertschen Zahlen L der höheren Verzweigungsgruppen die Art, wie die Verzweigungsgruppe in der ganzen Trägheitsgruppe enthalten ist, bestimmt wird. Man kann dadurch von gewissen Verzweigungskörpern direkt zeigen, daß die zugehörige Klassengruppe genau vom Index l ist.

Eingegangen 25. Juli 1939.

p-Sylowgruppen und p-Faktorgruppen.

Von *Helmut Wielandt* in Tübingen.

Burnside hat den Satz bewiesen: Liegt eine Sylowgruppe $\mathfrak{P}$ der endlichen Gruppe $\mathfrak{G}$ im Zentrum ihres eigenen Normalisators, so besitzt $\mathfrak{G}$ einen Normalteiler, dessen Faktorgruppe zu $\mathfrak{P}$ isomorph ist[1]). Der Beweis beruht auf der Verwendung monomialer Darstellungen. Die Methode ist von Burnside selbst[2]) und in den letzten Jahren von verschiedenen Verfassern zur Herleitung ähnlicher Ergebnisse unter schwächeren Voraussetzungen benutzt worden. Die vorliegende Arbeit hat dasselbe Ziel; sie ist entstanden durch den Versuch, einen Ansatz Burnsides möglichst weit auszunützen. Bei diesem Ansatz werden die Faktoren einer monomialen Substitution in gewisser Weise zu je p zusammengefaßt. Das Ergebnis ist ein umfassender, aber nicht ganz kurz auszusprechender Satz (Satz 1). Es zeigt vor allem, daß die bisher unter der Voraussetzung der Kommutativität gewisser Unter- und Faktorgruppen von $\mathfrak{P}$ hergeleiteten Ergebnisse schon unter der weit schwächeren der Regularität im Sinne von P. Hall gelten. Z. B. weiß man, daß im Falle einer abelschen p-Sylowgruppe $\mathfrak{P}$ die maximale p-Faktorgruppe von $\mathfrak{G}$ zu derjenigen des Normalisators von $\mathfrak{P}$ isomorph ist[3]); diese Behauptung gilt schon, wenn $\mathfrak{P}$ regulär ist (Satz 5). Hieraus folgt, da die Ordnung einer irregulären p-Gruppe $\geqq p^{p+1}$ ist: Ist die Ordnung von $\mathfrak{G}$ nicht durch p^{p+1} teilbar, so ist die maximale p-Faktorgruppe von $\mathfrak{G}$ isomorph zu derjenigen des Normalisators einer p-Sylowgruppe von $\mathfrak{G}$. Ein Beispiel (S. 192) zeigt, daß die Schranke p^{p+1} nicht mehr erhöht werden kann.

Ein anderer Spezialfall des Hauptsatzes besagt: Bilden die in einer p-Sylowgruppe von $\mathfrak{G}$ gelegenen Lösungen der Gleichung $X^p = E$, wobei E das Einheitselement bedeutet, eine Gruppe $\mathfrak{P}_1$, so ist die maximale abelsche p-Faktorgruppe von $\mathfrak{G}$ isomorph zu derjenigen des Normalisators von $\mathfrak{P}_1$.

Erwähnt werde noch die Bestimmung der Sylowgruppen gewisser höherer Kommutatorgruppen von $\mathfrak{G}$ (Satz 7) und die Ermittlung der Bedingungen, unter denen eine vorgelegte p-Untergruppe von $\mathfrak{G}$ als Sylowgruppe eines Normalteilers von $\mathfrak{G}$ auftreten kann, dessen Index eine Potenz von p ist (Satz 9).

I. Vorbemerkungen, Bezeichnungen.

a) Unter einer monomialen Substitution von n Variablen wird im folgenden eine Substitution

$$A = \begin{pmatrix} x_\nu \\ \varepsilon_\nu x_{\nu'} \end{pmatrix} \qquad (\nu = 1, 2, \ldots, n)$$

[1]) W. Burnside, On some properties of groups of odd order. II., Proc. London math. Soc. **33** (1901), 257—268.
[2]) A. a. O. [1]), 262—265.
[3]) O. Grün, Beiträge zur Gruppentheorie. I., J. reine angew. Math. **174** (1935), 1—14, Satz 6.

verstanden, wobei ν' die Zahlen $1, 2, \ldots, n$ in irgendeiner Reihenfolge durchläuft und die Faktoren ε_ν von Null verschiedene komplexe Zahlen sind. Wir setzen $\prod_{\nu=1}^{n} \varepsilon_\nu = \Delta(A)$; führt man zwei Substitutionen A, B nacheinander aus, so wird

$$\Delta(AB) = \Delta(A)\Delta(B).$$

Stimmt ein ν mit ν' überein, so sagen wir, x_ν sei fest bei A und werde von A mit dem Faktor ε_ν versehen, und ε_ν heißt dann ein Diagonalfaktor von A. Sind alle Variablen bei A fest, so heißt A eine Diagonalsubstitution.

b) Definition. Eine transitive Gruppe $\mathfrak{T}$ monomialer Substitutionen von p Variablen (p Primzahl) wird im folgenden kurz als eine *Ausnahmegruppe* bezeichnet, wenn ihre Ordnung eine Potenz von p ist und wenn in ihr eine Diagonalsubstitution D enthalten ist, deren sämtliche Faktoren ε_ν p-te Einheitswurzeln sind mit $\prod_{\nu=1}^{n} \varepsilon_\nu = \Delta(D) \neq 1$.

Der folgende Hilfssatz rechtfertigt die Bezeichnung „Ausnahmegruppe“:

Hilfssatz 1. *Jede Ausnahmegruppe ist irregulär.*

Zum Beweis ist an die Definition der Regularität zu erinnern[4]). Eine p-Gruppe heißt regulär, wenn für je zwei ihrer Elemente P, Q und jedes natürliche α eine Gleichung der Gestalt

$$(PQ)^{p^\alpha} = P^{p^\alpha} Q^{p^\alpha} S_1^{p^\alpha} S_2^{p^\alpha} \cdots$$

besteht, wobei die S_i der Kommutatorgruppe der von P und Q erzeugten Gruppe $\{P, Q\}$ angehören.

$\mathfrak{T}$ enthält, als transitive Gruppe, eine Nichtdiagonalsubstitution N; N besteht aus einem Zyklus des Grades p. Die Kommutatorgruppe der von N und der Ausnahmesubstitution D erzeugten Gruppe enthält nur Elemente S_i von derselben Gestalt wie D, nämlich Diagonalsubstitutionen, deren Faktoren p-te Einheitswurzeln sind. Daher sind alle $S_i^p = D^p = E$, und die Regularität von $\mathfrak{T}$ würde erfordern, daß $(DN)^p = N^p$ ist. Man rechnet aber leicht nach, daß $(DN)^p$ aus N^p durch Multiplikation mit dem Faktor $\Delta(D)$ hervorgeht, der nach Voraussetzung $\neq 1$ ist.

Wir legen jetzt die Voraussetzung fest, die in dieser Arbeit an die Stelle der bisher üblichen der Kommutativität tritt.

Definition. Eine p-Gruppe $\mathfrak{P}$ besitzt *die Eigenschaft R*, wenn unter den monomialen Substitutionsgruppen, welche Darstellungen von Untergruppen von $\mathfrak{P}$ sind, keine Ausnahmegruppe auftritt. (Dabei gilt, wie üblich, auch $\mathfrak{P}$ als Untergruppe von $\mathfrak{P}$.)

Da alle Unter- und Faktorgruppen einer regulären Gruppe regulär sind, besitzt nach Hilfssatz 1 jede reguläre p-Gruppe die Eigenschaft R, insbesondere jede abelsche.

c) $\mathfrak{H}$ sei eine transitive Permutationsgruppe, deren Ordnung eine Potenz der Primzahl p ist; $\mathfrak{A} \neq E$ sei ein Normalteiler von $\mathfrak{H}$. Dann enthält bekanntlich[5]) $\mathfrak{A}$ ein Element A der Ordnung p, das mit jedem Element H von $\mathfrak{H}$ vertauschbar ist. Daher werden die bei H festen Variablen (falls es solche überhaupt gibt) von A nur untereinander permutiert, und zwar zyklisch zu je p; denn weil $\mathfrak{H}$ transitiv und A im Zentrum von $\mathfrak{H}$ ist, haben alle Zyklen von A denselben Grad p.

Diese Überlegung wenden wir nun, wenn $\mathfrak{R}$ eine transitive monomiale p-Gruppe bedeutet, auf die Permutationsgruppe an, die aus $\mathfrak{R}$ entsteht, wenn alle Faktoren ε_ν durch 1 ersetzt werden. So erhalten wir den

---

[4]) P. Hall, A contribution to the theory of groups of prime-power orders, Proc. London math. Soc. (2) **36** (1933), 29—95, Definition 4.11.

[5]) Vgl. z. B. J.-A. de Séguier, Éléments de la théorie des groupes abstraits (Paris 1904), 63.

Hilfssatz 2. *$\mathfrak{K}$ sei eine transitive p-Gruppe monomialer Substitutionen; $\mathfrak{A}$ sei ein Normalteiler von $\mathfrak{K}$, der nicht nur aus Diagonalsubstitutionen besteht. Dann enthält $\mathfrak{A}$ ein Element A mit der Eigenschaft: Alle Zyklen von A haben den Grad p; ist eine Variable bei einem Element $K < \mathfrak{K}$ fest, so sind bei K auch die $p-1$ übrigen Variablen fest, die demselben Zyklus von A angehören.*

d) Wir führen einen Begriff ein, der sich auf abstrakte Gruppen bezieht, aber mit monomialen Darstellungen zusammenhängt; dabei benützen wir für $B^{-1}AB$ die Schreibweise A^B.

Definition. $\mathfrak{A}$ und $\mathfrak{H}$ seien Untergruppen von $\mathfrak{G}$, und es sei $\mathfrak{A} < \mathfrak{H}$. Dann heißt

α) $\mathfrak{A}$ (bezüglich $\mathfrak{G}$) *stark abgeschlossen* in $\mathfrak{H}$, wenn für jedes Element $G < \mathfrak{G}$ der Durchschnitt von $\mathfrak{A}^G$ mit $\mathfrak{H}$ in $\mathfrak{A}$ liegt: $\mathfrak{A}^G \cap \mathfrak{H} < \mathfrak{A}$;

β) $\mathfrak{A}$ (bezüglich $\mathfrak{G}$) *schwach abgeschlossen* in $\mathfrak{H}$, wenn $\mathfrak{H}$ keine zu $\mathfrak{A}$ in $\mathfrak{G}$ konjugierte Gruppe enthält, abgesehen von $\mathfrak{A}$ selbst: aus $\mathfrak{A}^G < \mathfrak{H}$ folgt $\mathfrak{A}^G = \mathfrak{A}$.

Aus dieser Definition folgen unmittelbar die Regeln:

Ist $\mathfrak{A}$ stark abgeschlossen in $\mathfrak{H}$, dann auch schwach. Sind $\mathfrak{A}_1$ und $\mathfrak{A}_2$ stark abgeschlossen in $\mathfrak{H}$, dann auch ihr Durchschnitt $\mathfrak{A}_1 \cap \mathfrak{A}_2$. Sind $\mathfrak{A}_1$ und $\mathfrak{A}_2$ schwach abgeschlossen in $\mathfrak{H}$, dann auch ihr Erzeugnis $\{\mathfrak{A}_1, \mathfrak{A}_2\}$. Ist $\mathfrak{A}$ stark oder schwach abgeschlossen in $\mathfrak{H}$, dann ist $\mathfrak{A}$ ein Normalteiler des Normalisators von $\mathfrak{H}$.

Beispiele abgeschlossener Gruppen: Die Untergruppe von $\mathfrak{H}$, die von den in $\mathfrak{H}$ gelegenen Lösungen einer Gleichung $X^k = E$ erzeugt wird, ist schwach abgeschlossen in $\mathfrak{H}$. Falls diese Lösungen schon selber eine Gruppe bilden, ist sie sogar stark abgeschlossen; dieser Fall tritt z. B. dann ein, wenn $\mathfrak{H}$ eine reguläre p-Gruppe ist[6]). Ferner ist der Durchschnitt von $\mathfrak{H}$ mit einem Normalteiler von $\mathfrak{G}$ stark abgeschlossen.

Für das Folgende ist der Fall wichtig, daß $\mathfrak{H}$ eine Sylowgruppe von $\mathfrak{G}$ ist. Es gilt das Kriterium, das übrigens im folgenden nicht benützt wird: Die Untergruppe $\mathfrak{A}$ der Sylowgruppe $\mathfrak{P}$ von $\mathfrak{G}$ ist dann und nur dann schwach abgeschlossen in $\mathfrak{P}$, wenn der Normalisator von $\mathfrak{A}$ sowohl den Normalisator von $\mathfrak{P}$ wie die sämtlichen $\mathfrak{A}$ enthaltenden zu $\mathfrak{P}$ konjugierten Gruppen $\mathfrak{P}^G$ enthält. Der Beweis dieses Kriteriums ist nach einer geläufigen Schlußweise[7]) leicht zu führen.

Grün und Zappa haben Sonderfälle dieser Begriffe eingeführt. Sie laufen auf folgendes hinaus: Grün bezeichnet die Gruppe $\mathfrak{G}$ als p-normal, wenn das Zentrum $\mathfrak{Z}$ einer p-Sylowgruppe $\mathfrak{P}$ schwach abgeschlossen in $\mathfrak{P}$ ist[8]), und er bezeichnet $\mathfrak{G}$ als p-normal für eine Untergruppe $\mathfrak{A}$ von $\mathfrak{P}$, wenn $\mathfrak{A}$ in $\mathfrak{P}$ stark abgeschlossen ist[9]). Zappa[10]) nennt eine Untergruppe $\mathfrak{A}$ von $\mathfrak{P}$ kanonisch, wenn sie in $\mathfrak{P}$ schwach abgeschlossen ist.

Ist $\mathfrak{A}$ eine beliebige Untergruppe von $\mathfrak{H}$, so bezeichnen wir das Erzeugnis aller zu $\mathfrak{A}$ in $\mathfrak{G}$ konjugierten Untergruppen $\mathfrak{A}^G$, welche in $\mathfrak{H}$ liegen, als die *schwache Abschließung von* $\mathfrak{A}$ in $\mathfrak{H}$, und das Erzeugnis aller Durchschnitte $\mathfrak{A}^G \cap \mathfrak{H}$ als die *starke Abschließung von* $\mathfrak{A}$ in $\mathfrak{H}$. Die schwache Abschließung ist schwach abgeschlossen.

e) Daß diese Begriffe mit der Theorie der monomialen Darstellungen zusammenhängen, zeigen die beiden folgenden Hilfssätze:

---

[6]) A. a. O. [4]), Satz 4.26.

[7]) Vgl. z. B. A. Speiser, Die Theorie der Gruppen von endlicher Ordnung, 2. Aufl. (Berlin 1927), Satz 75.

[8]) A. a. O. [3]), 3.

[9]) O. Grün, Gruppentheoretische Untersuchungen, Deutsche Math. **3** (1938), 547—555, 550.

[10]) G. Zappa, Un criterio di non semplicità per i gruppi finiti, Rend. Sem. mat. Univ. Roma (4) **2** (1938), 173—176.

Hilfssatz 3. *$\mathfrak{A}$ und $\mathfrak{H}$ seien Untergruppen von $\mathfrak{G}$. $\mathfrak{A}$ sei schwach abgeschlossen in $\mathfrak{H}$, und $\mathfrak{H}$ enthalte den Normalisator von $\mathfrak{A}$ in $\mathfrak{G}$. Stellt man dann $\mathfrak{G}$ mit Hilfe von $\mathfrak{H}$ monomial dar (als transitive Gruppe des Grades $(\mathfrak{G}:\mathfrak{H})$), so wird $\mathfrak{A}$ durch eine intransitive monomiale Gruppe dargestellt, die genau einen transitiven Konstituenten des Grades 1 hat.*

Beweis. Nach Konstruktion der Darstellung[11]) ist $\mathfrak{H}$ die größte Untergruppe von $\mathfrak{G}$, bei welcher eine gewisse Variable, etwa x_1, fest ist. Also ist x_1 insbesondere bei $\mathfrak{A}$ fest. Nun sei z. B. x_ν bei $\mathfrak{A}$ fest. Wir wählen ein Element $G < \mathfrak{G}$, welches x_ν in $\gamma_\nu x_1$ überführt. Bei $\mathfrak{A}^G$ ist dann x_1 fest, also ist $\mathfrak{A}^G < \mathfrak{H}$. Wegen der Abgeschlossenheit von $\mathfrak{A}$ ist $\mathfrak{A}^G = \mathfrak{A}$; also liegt G im Normalisator von $\mathfrak{A}$, mithin nach Voraussetzung in $\mathfrak{H}$. Das besagt, daß $\nu = 1$ ist.

Hilfssatz 4. *$\mathfrak{G}$ werde mit Hilfe der Untergruppe $\mathfrak{H}$ monomial dargestellt (als transitive Gruppe des Grades $(\mathfrak{G}:\mathfrak{H})$); bei $\mathfrak{H}$ sei x_1 fest, und $\overline{\mathfrak{H}}$ sei der Normalteiler derjenigen Elemente von $\mathfrak{H}$, von denen x_1 mit dem Faktor 1 versehen wird; $\mathfrak{A}$ sei eine Untergruppe von $\mathfrak{H}$. Falls $\overline{\mathfrak{H}}$ die starke Abschließung von $\mathfrak{A}$ in $\mathfrak{H}$ enthält, so ist $\Delta(Z) = 1$ für jeden einzelnen Zyklus Z eines beliebigen Elements $A < \mathfrak{A}$. Dabei gelten Diagonalfaktoren als Zyklen des Grades 1.*

Beweis. Wir betrachten zuerst die Zyklen des Grades 1. Es sei ε_ν ein Diagonalfaktor von A. Wählen wir ein Element $G < \mathfrak{G}$, welches x_ν in $\gamma_\nu x_1$ überführt, so ist x_1 bei A^G fest und wird mit dem Faktor ε_ν versehen. Insbesondere ist $A^G < \mathfrak{H}$. Nach Definition gehört A^G der starken Abschließung von $\mathfrak{A}$ in $\mathfrak{H}$ an, daher ist nach Voraussetzung $A^G < \mathfrak{H}$. Das besagt, daß $\varepsilon_\nu = 1$ ist.

Nun sei Z ein Zyklus des Grades $k > 1$ von A. Wie man leicht nachrechnet, ist Z^k die Diagonalsubstitution des Grades k, in der alle Faktoren den Wert $\Delta(Z)$ haben. Anderseits ist Z^k eine Teilsubstitution des Elements $A^k < \mathfrak{A}$. Daher ist $\Delta(Z) = 1$.

f) Im folgenden bedeutet p eine feste Primzahl. Wo von Sylowgruppen die Rede ist, sind solche gemeint, deren Ordnung eine Potenz von p ist.

II. Der Hauptsatz.

Der Hauptsatz lautet:

Satz 1. *$\mathfrak{P}$ sei eine p-Sylowgruppe von $\mathfrak{G}$, $\mathfrak{P}_1$ sei schwach abgeschlossen in $\mathfrak{P}$. $\mathfrak{N}$ sei der Normalisator von $\mathfrak{P}_1$ in $\mathfrak{G}$, $\overline{\mathfrak{N}}$ ein Normalteiler von $\mathfrak{N}$ mit abelscher p-Faktorgruppe $\mathfrak{N}/\overline{\mathfrak{N}}$.*

$\mathfrak{G}$ besitzt einen Normalteiler $\overline{\mathfrak{G}}$ mit $\overline{\mathfrak{G}} \cap \mathfrak{N} = \overline{\mathfrak{N}}$ und $\overline{\mathfrak{G}}\mathfrak{N} = \mathfrak{G}$ (also insbesondere $\mathfrak{G}/\overline{\mathfrak{G}} \simeq \mathfrak{N}/\overline{\mathfrak{N}}$), falls es in $\mathfrak{P}$ zwei Untergruppen $\mathfrak{P}_0$ und $\mathfrak{P}_2$ mit den folgenden Eigenschaften gibt:

$\mathfrak{P}_0$ ist stark abgeschlossen in $\mathfrak{P}$,

$\mathfrak{P}_1$ und $\mathfrak{P}_2$ sind Normalteiler von $\mathfrak{P}_0$,

für je zwei Elemente $P_0 < \mathfrak{P}_0$ und $P_1 < \mathfrak{P}_1$ besitzt die Faktorgruppe $\{P_0, P_1, \mathfrak{P}_2\}/\mathfrak{P}_2$ die Eigenschaft R,

die starke Abschließung von $\mathfrak{P}_2$ in $\mathfrak{P}$ liegt in $\overline{\mathfrak{N}}$.

Wir führen den Beweis zuerst für den Fall einer zyklischen Faktorgruppe $\mathfrak{N}/\overline{\mathfrak{N}}$; am Schluß des Abschnitts wird der allgemeine abelsche Fall auf diesen zurückgeführt. In Abschnitt IV wird der Satz auf nichtabelsche Faktorgruppen übertragen werden.

Wir stellen $\mathfrak{G}$ mit Hilfe von $\mathfrak{N}$ und $\overline{\mathfrak{N}}$ homomorph als monomiale Substitutionsgruppe des Grades $(\mathfrak{G}:\mathfrak{N}) = n$ dar; die Faktoren der Substitutionen sind $(\mathfrak{N}:\overline{\mathfrak{N}})$-te Einheitswurzeln. Wir bezeichnen die Variablen so, daß x_1 genau bei $\mathfrak{N}$ fest ist und genau von $\overline{\mathfrak{N}}$ mit dem Faktor 1 versehen wird. Wir behaupten der Reihe nach:

---

[11]) A. a. O. [7]), 139—140.

(a) In dieser monomialen Darstellung von $\mathfrak{G}$ besitzt $\mathfrak{P}_1$ keinen transitiven Konstituenten des Grades 1 außer dem auf x_1 bezüglichen.

Das folgt aus Hilfssatz 3, sobald wir nachgeprüft haben, daß $\mathfrak{P}_1$ in $\mathfrak{N}$ schwach abgeschlossen ist. $\mathfrak{P}_1$ ist schwach abgeschlossen in $\mathfrak{P}$, daher invariant in $\mathfrak{P}$. Also ist $\mathfrak{P}$ eine Sylowgruppe von $\mathfrak{N}$. Wenn nun $\mathfrak{P}_1^G < \mathfrak{N}$ ist, ist nach den Sylowschen Sätzen $\mathfrak{P}_1^{GN} < \mathfrak{P}$ für ein geeignetes $N < \mathfrak{N}$. Es ergibt sich $\mathfrak{P}_1^{GN} = \mathfrak{P}_1$ und damit $\mathfrak{P}_1^G = \mathfrak{P}_1$. Also ist $\mathfrak{P}_1$ in $\mathfrak{N}$ schwach abgeschlossen.

(b) Man kann die von x_1 verschiedenen Variablen $x_2, x_3, \ldots, x_n$ derart in Systeme $\mathfrak{S}^{(1)}, \mathfrak{S}^{(2)}, \ldots, \mathfrak{S}^{\left(\frac{n-1}{p}\right)}$ zu je p einteilen, daß bei einem Element $P < \mathfrak{P}$, bei welchem eine Variable von $\mathfrak{S}^{(\alpha)}$ fest ist, auch die $p-1$ übrigen fest sind, und daß P mit einem geeigneten Element $P_1^{(\alpha)} < \mathfrak{P}_1$ zusammen eine Gruppe $\{P, P_1^{(\alpha)}\}$ erzeugt, welche in den p Variablen von $\mathfrak{S}^{(\alpha)}$ einen transitiven Konstituenten $\mathfrak{T}^{(\alpha)}$ des Grades p besitzt.

Beweis. Die transitiven Konstituenten von $\mathfrak{P}$ seien $\mathfrak{K}_1, \mathfrak{K}_2, \ldots, \mathfrak{K}_r$. $\mathfrak{K}_1$ beziehe sich auf x_1; für die übrigen $\mathfrak{K}_\varrho$ ist nach **(a)** der Grad $k_\varrho > 1$, da $\mathfrak{P}_1 < \mathfrak{P}$ ist. $\mathfrak{K}_\varrho$ ist eine Darstellung von $\mathfrak{P}$; das Bild von $\mathfrak{P}_1$ in dieser Darstellung ist ein Normalteiler $\mathfrak{A}_\varrho$ von $\mathfrak{K}_\varrho$, der nach **(a)** nicht nur aus Diagonalsubstitutionen besteht. Nach Hilfssatz 2 enthält $\mathfrak{A}_\varrho$ ein Element A_ϱ mit der Eigenschaft: Alle Zyklen von A_ϱ haben den Grad p; ist eine Variable bei einem Element $K_\varrho < \mathfrak{K}_\varrho$ fest, so sind bei K_ϱ auch die $p-1$ übrigen Variablen fest, die demselben Zyklus von A_ϱ angehören. Wir teilen die k_ϱ Variablen von $\mathfrak{K}_\varrho$ in die $\frac{k_\varrho}{p}$ Transitivitätssysteme von A_ϱ ein. Bezeichnen wir die insgesamt für $\varrho = 2, 3, \ldots, r$ auf diese Weise entstehenden Transitivitätssysteme mit $\mathfrak{S}^{(1)}, \mathfrak{S}^{(2)}, \ldots, \mathfrak{S}^{\left(\frac{n-1}{p}\right)}$ und verstehen wir unter $P_1^{(\alpha)}$ ein Element von $\mathfrak{P}_1$, welches das für $\mathfrak{S}^{(\alpha)}$ verantwortliche A_ϱ als Konstituenten in $\mathfrak{K}_\varrho$ besitzt, so ist die gewünschte Konstruktion geleistet.

(c) Ist $P_0 < \mathfrak{P}_0$, so ist der in **(b)** erwähnte transitive Konstituent $\mathfrak{T}^{(\alpha)}$ des Grades p der Gruppe $\{P_0, P_1^{(\alpha)}\}$ keine Ausnahmegruppe.

Beweis. Diejenigen Elemente der Gruppe $\{P_0, P_1^{(\alpha)}\} = \mathfrak{Q}$, die als Konstituenten in $\mathfrak{T}^{(\alpha)}$ die identische Substitution besitzen, bilden einen Normalteiler $\overline{\mathfrak{Q}}$ von $\mathfrak{Q}$. Wir unterscheiden die zwei Fälle, ob $\mathfrak{P}_2 \cap \mathfrak{Q} < \overline{\mathfrak{Q}}$ ist oder nicht.

Ist $\mathfrak{P}_2 \cap \mathfrak{Q} < \overline{\mathfrak{Q}}$, so ist $\mathfrak{Q}/\overline{\mathfrak{Q}}$ eine Faktorgruppe von $\mathfrak{Q}/\mathfrak{P}_2 \cap \mathfrak{Q}$, also isomorph zu einer Faktorgruppe von $\mathfrak{P}_2\mathfrak{Q}/\mathfrak{P}_2 = \{P_0, P_1^{(\alpha)}, \mathfrak{P}_2\}/\mathfrak{P}_2$. Da diese Gruppe nach Voraussetzung die Eigenschaft R besitzt, ist $\mathfrak{T}^{(\alpha)}$ keine Ausnahmegruppe.

Ist dagegen $\mathfrak{P}_2 \cap \mathfrak{Q} \not< \overline{\mathfrak{Q}}$, d. h. besitzt $\mathfrak{P}_2 \cap \mathfrak{Q}$ als Konstituenten in $\mathfrak{T}^{(\alpha)}$ nicht nur die identische Substitution, so benützen wir die Voraussetzung, daß $\overline{\mathfrak{N}}$ die starke Abschließung von $\mathfrak{P}_2$ in $\mathfrak{P}$ enthält. Wir schließen daraus wie in **(a)**, daß $\overline{\mathfrak{N}}$ auch die starke Abschließung von $\mathfrak{P}_2$ in $\mathfrak{N}$ enthält. Daher ist nach Hilfssatz 4, auf $\mathfrak{G}$, $\mathfrak{N}$, $\overline{\mathfrak{N}}$ und $\mathfrak{P}_2$ angewandt, jeder Diagonalfaktor eines beliebigen Elements von $\mathfrak{P}_2$ gleich 1. Das gilt insbesondere für die Elemente von $\mathfrak{P}_2 \cap \mathfrak{Q}$; daher hat ein solches Element als Konstituenten in $\mathfrak{T}^{(\alpha)}$ die identische Substitution, sobald auch nur eine der Variablen von $\mathfrak{S}^{(\alpha)}$ bei ihm fest ist. Das zeigt, daß die Ordnung des Konstituenten von $\mathfrak{P}_2 \cap \mathfrak{Q}$ in $\mathfrak{T}^{(\alpha)}$ gleich seinem Grad p ist. Da dieser Konstituent ein Normalteiler von $\mathfrak{T}^{(\alpha)}$ ist, liegt er im Zentrum von $\mathfrak{T}^{(\alpha)}$. Da er nicht nur aus Diagonalsubstitutionen besteht, ist $\mathfrak{T}^{(\alpha)}$ abelsch. Also ist $\mathfrak{T}^{(\alpha)}$ keine Ausnahmegruppe.

(d) Das Element $P_0 < \mathfrak{P}_0$ versehe die Variable x_1 mit dem Faktor ε_1. Die außer ε_1 eventuell noch vorhandenen Diagonalfaktoren von P_0 seien p-te Einheitswurzeln. Dann ist das Produkt aller Diagonalfaktoren von P_0 gleich ε_1.

Beweis. Wir teilen die Variablen $x_2, x_3, \ldots, x_n$ in die unter **(b)** beschriebenen Systeme $\mathfrak{S}^{(\alpha)}$ zu je p ein und bilden für diejenigen $\mathfrak{S}^{(\alpha)}$, deren Variablen bei P_0 fest sind, die transitiven Konstituenten $\mathfrak{T}^{(\alpha)}$. Da $\mathfrak{T}^{(\alpha)}$ nach **(c)** keine Ausnahmegruppe ist, ist das Produkt der p Diagonalfaktoren von P_0 in $\mathfrak{T}^{(\alpha)}$ gleich 1. Multipliziert man über die $\mathfrak{T}^{(\alpha)}$, so ergibt sich die Behauptung.

Mit dem nächsten Schritt gehen wir über den Ansatz von Burnside[2]) hinaus. Bisher haben wir die Voraussetzung, daß $\mathfrak{P}_0$ in $\mathfrak{P}$ stark abgeschlossen ist, nicht herangezogen. Tun wir dies jetzt, so können wir zeigen:

(e) Es sei $P_0 < \mathfrak{P}_0$. Falls alle Diagonalfaktoren von P_0 p-te Einheitswurzeln sind, stimmen sie sämtlich miteinander überein.

Beweis. P_0 versehe x_1 mit dem Faktor ε_1 und eine andere Variable x_ν mit dem Faktor ε_ν. Das Produkt aller Diagonalfaktoren von P_0 hat nach **(d)** den Wert ε_1. Wir zeigen, daß es anderseits gleich ε_ν ist. Wir wählen ein $G < \mathfrak{G}$, welches x_ν in $\gamma_\nu x_1$ überführt. Dann liegt $P_0^G < \mathfrak{N}$. Wir können daher mit einem $N < \mathfrak{N}$ transformieren, so daß $P_0^{GN} < \mathfrak{P}$ ist. Da $\mathfrak{P}_0$ in $\mathfrak{P}$ stark abgeschlossen ist, liegt $P_0' = P_0^{GN} < \mathfrak{P}_0$, und wir können **(d)** auf P_0' anwenden. Die Diagonalfaktoren von P_0' sind bis auf die Anordnung dieselben wie die von P_0, und P_0' versieht x_1 mit dem Faktor ε_ν. Also ist das Produkt aller Diagonalfaktoren von P_0 gleich ε_ν.

(f) Jeder Diagonalfaktor des Elements $P_0 < \mathfrak{P}_0$ ist gleich 1, wenn auch nur einer von ihnen gleich 1 ist.

Beweis. Andernfalls hätte eine geeignete Potenz P_0^k Diagonalfaktoren, die sämtlich p-te Einheitswurzeln sind, aber nicht alle mit 1 übereinstimmen. Dem widerspricht **(e)**.

(g) Das Element $P_0 < \mathfrak{P}_0$ versehe x_1 mit dem Faktor ε_1. Wenn ε_1 eine p-te Einheitswurzel ist, hat das Produkt aller Faktoren von P_0 den Wert $\Delta(P_0) = \varepsilon_1$.

Beweis. Zunächst folgt, indem man **(f)** auf P_0^p anwendet, daß jeder Diagonalfaktor von P_0 eine p-te Einheitswurzel ist. Nach **(d)** ist das Produkt der Diagonalfaktoren gleich ε_1. Wir brauchen daher nur noch zu zeigen, daß für jeden einzelnen Zyklus Z des Grades $k = p^\varkappa > 1$ von P_0 $\Delta(Z) = 1$ ist. Das ergibt sich aber, wenn man **(f)** auf P_0^k anwendet; denn P_0^k versieht x_1 mit dem Faktor $\varepsilon_1^k = 1$ und die von Z betroffenen Variablen mit dem Faktor $\Delta(Z)$.

(h) Das Element $P_0 < \mathfrak{P}_0$ versehe x_1 mit dem Faktor ε_1. Dann und nur dann ist $\Delta(P_0) = 1$, wenn $\varepsilon_1 = 1$ ist.

Beweis. Daß aus $\varepsilon_1 = 1$ auch $\Delta(P_0) = 1$ folgt, haben wir schon unter **(g)** bewiesen. Daß aus $\Delta(P_0) = 1$ auch $\varepsilon_1 = 1$ folgt, beweisen wir indirekt: Andernfalls wäre eine geeignete Potenz ε_1^k eine primitive p-te Einheitswurzel, also müßte nach **(g)** $\Delta(P_0^k) = \varepsilon_1^k \neq 1$ sein, während nach Voraussetzung $\Delta(P_0^k) = \Delta(P_0)^k = 1$ ist.

Nach **(h)** versehen zwei Elemente $P_0, P_0' < \mathfrak{P}_0$, für die $\Delta(P_0) = \Delta(P_0')$ ist, x_1 mit demselben Faktor. Hieraus folgt, wenn man die Gleichung $\Delta(P_0^G) = \Delta(P_0)$ beachtet, wie in **(e)**:

(i) Für ein Element $P_0 < \mathfrak{P}_0$ stimmen alle Diagonalfaktoren miteinander überein.

Dieses Ergebnis kann auf die höheren Zyklen in der folgenden Form ausgedehnt werden:

(j) Das Element $P_0 < \mathfrak{P}_0$ versehe x_1 mit dem Faktor ε_1. Für jeden Zyklus Z des Grades k von P_0 gilt dann $\Delta(Z) = \varepsilon_1^k$.

Beweis. P_0^k versieht x_1 mit dem Faktor ε_1^k und die von Z betroffenen Variablen mit dem Faktor $\Delta(Z)$.

Damit wissen wir über die der Untergruppe $\mathfrak{P}_0$ von $\mathfrak{P}$ entsprechenden Substitutionen unserer Darstellung genügend genau Bescheid. Wir übertragen jetzt die Ergebnisse auf $\mathfrak{P}$:

(k) Die Behauptung **(j)** gilt für alle Elemente $P < \mathfrak{P}$.

Den Beweis führen wir durch vollständige Induktion nach der Relativordnung von P in bezug auf $\mathfrak{P}_0$, d. i. die kleinste natürliche Zahl m, für die $P^m < \mathfrak{P}_0$ ist. Der Fall $m = 1$ ist durch **(j)** erledigt. Im Fall $m > 1$ teilen wir die Zyklen Z von P danach ein, ob ihr Grad $k > 1$ oder $= 1$ ist.

Ist $k > 1$, so ist die Relativordnung von P^k kleiner als die von P. Also können wir **(k)** auf P^k schon anwenden. Wie bei **(j)** ergibt sich $\Delta(Z) = \varepsilon_1^k$.

Ist $k = 1$, so ziehen wir noch einmal die in **(b)** vorgenommene Einteilung der Variablen $x_2, x_3, \ldots, x_n$ in Systeme $\mathfrak{S}^{(\alpha)}$ zu je p heran. Wir behaupten: Sind bei P die Variablen von $\mathfrak{S}^{(\alpha)}$ fest, so ist das Produkt der zugehörigen p Diagonalfaktoren von P gleich ε_1^p. Zum Beweis betrachten wir den in **(b)** erwähnten Konstituenten $\mathfrak{T}^{(\alpha)}$ der Gruppe $\{P, P_1^{(\alpha)}\}$. Wir bezeichnen mit D_P den (Diagonal-)Konstituenten von P in $\mathfrak{T}^{(\alpha)}$, mit $Z_{P_1^{(\alpha)}}$ den (zyklischen) Konstituenten von $P_1^{(\alpha)}$ in $\mathfrak{T}^{(\alpha)}$ und mit η_1 den Faktor, mit welchem x_1 von $P_1^{(\alpha)}$ versehen wird. Dann ist

$$\Delta(D_P Z_{P_1^{(\alpha)}}) = (\varepsilon_1 \eta_1)^p, \qquad \Delta(Z_{P_1^{(\alpha)}}) = \eta_1^p.$$

Die erste Gleichung gilt nach dem schon bewiesenen Teil von **(k)**, weil $P P_1^{(\alpha)}$ ein Element derselben Relativordnung wie P ist, in $\mathfrak{T}^{(\alpha)}$ einen Zyklus des Grades $p > 1$ hat und x_1 mit dem Faktor $\varepsilon_1 \eta_1$ versieht. Die zweite gilt nach **(j)**, weil $P_1^{(\alpha)} < \mathfrak{P}_1 < \mathfrak{P}_0$ ist. Aus beiden Gleichungen zusammen folgt $\Delta(D_P) = \varepsilon_1^p$, d. h. das Produkt der Diagonalfaktoren von P in $\mathfrak{T}^{(\alpha)}$ ist tatsächlich, wie unsere Teilbehauptung besagt, ε_1^p.

Multiplizieren wir über diejenigen $\mathfrak{T}^{(\alpha)}$, deren Variablen bei P fest sind, so ergibt sich: Das Produkt aller Diagonalfaktoren von P ist $= \varepsilon_1^d$, wenn ihre Anzahl d ist. Anderseits ist dasselbe Produkt $= \varepsilon_\nu^d$, wobei ε_ν ein beliebiger Diagonalfaktor von P ist. Denn wählen wir ein $G < \mathfrak{G}$, welches x_ν in $\gamma_\nu x_1$ überführt, derart, daß $P^G < \mathfrak{P}$ ist, so versieht P^G die Variable x_1 mit dem Faktor ε_ν, und außerdem ist $(P^G)^m = (P^m)^G < \mathfrak{P}_0$, weil $P^m < \mathfrak{P}_0$ ist und $\mathfrak{P}_0$ nach Voraussetzung in $\mathfrak{P}$ stark abgeschlossen ist; auf P^G kann man daher das bisher Bewiesene anwenden: Das Produkt der Diagonalfaktoren von P^G, d. h. das Produkt der Diagonalfaktoren von P, hat den Wert ε_ν^d, wie behauptet.

Nun ergibt sich für die Zyklen des Grades 1 die Aussage von **(k)**: $\varepsilon_\nu = \varepsilon_1$. Denn es ist $\varepsilon_\nu^d = \varepsilon_1^d$ und $d \equiv 1 \pmod p$.

Es folgt:

(l) Das Element $N < \mathfrak{N}$ versehe x_1 mit dem Faktor ε_1. Dann hat das Produkt aller Faktoren von N den Wert $\Delta(N) = \varepsilon_1^n$ mit $n = (\mathfrak{G} : \mathfrak{N})$.

Beweis. Liegt $N < \mathfrak{P}$, so ergibt sich **(l)** unmittelbar aus **(k)**, indem man über alle Zyklen von N multipliziert. Ist $N \not< \mathfrak{P}$, ist aber die Ordnung von N eine Potenz von p, so wählen wir ein $T < \mathfrak{N}$ derart, daß $N^T < \mathfrak{P}$ ist; dann ist $\Delta(N) = \Delta(N^T)$, also gleich der n-ten Potenz des Faktors, mit dem N^T die Variable x_1 versieht; dieser Faktor ist ε_1, weil x_1 bei T fest ist; also ist auch in diesem Fall $\Delta(N) = \varepsilon_1^n$. Ist schließlich N ein beliebiges

Element von $\mathfrak{N}$, so ist für einen geeigneten zu p teilerfremden Exponenten q die Ordnung von N^q eine Potenz von p; es wird $\Delta(N)^q = \Delta(N^q) = \varepsilon_1^{qn}$, also $\Delta(N) = \varepsilon_1^n$.

(m) Die Elemente $\overline{G} < \mathfrak{G}$ mit $\Delta(\overline{G}) = 1$ bilden einen Normalteiler $\overline{\mathfrak{G}}$ mit $\overline{\mathfrak{G}} \cap \mathfrak{N} = \overline{\mathfrak{N}}$ und $\overline{\mathfrak{G}}\mathfrak{N} = \mathfrak{G}$.

Beweis. Sie bilden einen Normalteiler $\overline{\mathfrak{G}}$ wegen $\Delta(G_1 G_2) = \Delta(G_1)\,\Delta(G_2)$. Für ein Element $N < \mathfrak{N}$ ist nach **(l)** dann und nur dann $\Delta(N) = 1$, wenn x_1 von N mit dem Faktor $\varepsilon_1 = 1$ versehen wird, d. h. wenn $N < \overline{\mathfrak{N}}$ liegt. Da der Index $(\mathfrak{G} : \overline{\mathfrak{G}})$ eine Potenz von p ist und $\mathfrak{N}$ eine p-Sylowgruppe von $\mathfrak{G}$ enthält, ist $\overline{\mathfrak{G}}\mathfrak{N} = \mathfrak{G}$.

Damit ist der Hauptsatz für den Fall einer zyklischen Faktorgruppe $\mathfrak{N}/\overline{\mathfrak{N}}$ bewiesen. Falls $\mathfrak{N}/\overline{\mathfrak{N}}$ eine nichtzyklische abelsche p-Gruppe ist, bestimmen wir geeignete Normalteiler $\overline{\mathfrak{N}}_1, \overline{\mathfrak{N}}_2, \ldots$ von $\mathfrak{N}$ derart, daß $\mathfrak{N}/\overline{\mathfrak{N}}_i$ zyklisch und daß der Durchschnitt $\overline{\mathfrak{N}}_1 \cap \overline{\mathfrak{N}}_2 \cap \cdots = \overline{\mathfrak{N}}$ ist. Zu jedem $\overline{\mathfrak{N}}_i$ bestimmen wir nach dem Hauptsatz einen Normalteiler $\overline{\mathfrak{G}}_i$ von $\mathfrak{G}$ so, daß $\overline{\mathfrak{G}}_i \cap \mathfrak{N} = \overline{\mathfrak{N}}_i$ und $(\mathfrak{G} : \overline{\mathfrak{G}}_i) = (\mathfrak{N} : \overline{\mathfrak{N}}_i)$ ist, und setzen $\overline{\mathfrak{G}} = \overline{\mathfrak{G}}_1 \cap \overline{\mathfrak{G}}_2 \cap \cdots$. Es wird

$$\overline{\mathfrak{G}} \cap \mathfrak{N} = (\overline{\mathfrak{G}}_1 \cap \mathfrak{N}) \cap (\overline{\mathfrak{G}}_2 \cap \mathfrak{N}) \cap \cdots = \overline{\mathfrak{N}},$$

und aus demselben Grund wie bei **(m)** wird $\overline{\mathfrak{G}}\mathfrak{N} = \mathfrak{G}$. Damit ist der Beweis beendet[12]).

Der Inhalt des Satzes wird durchsichtiger werden, wenn wir zu einigen einfachen Sonderfällen Beispiele bilden. Das geschieht im nächsten Abschnitt. Wir ersetzen dabei zur Vereinfachung die Bedingung R durch die geläufigere der Regularität.

III. Grenzfälle des Hauptsatzes.

Die im Hauptsatz auftretenden Gruppen $\mathfrak{P}$, $\mathfrak{P}_0$, $\mathfrak{P}_1$, $\mathfrak{P}_2$ stehen in der Beziehung:

$$E < \mathfrak{P}_{1,2} < \mathfrak{P}_0 < \mathfrak{P}.$$

Wir betrachten vier Grenzfälle, die durch das Zusammenfallen einiger von ihnen entstehen.

(a) $\mathfrak{P}_2 = E$, $\mathfrak{P}_0 = \mathfrak{P}_1$. Der Hauptsatz besagt: $\mathfrak{P}$ sei eine Sylowgruppe von $\mathfrak{G}$, $\mathfrak{P}_1$ sei stark abgeschlossen in $\mathfrak{P}$. $\mathfrak{N}$ sei der Normalisator von $\mathfrak{P}_1$, $\overline{\mathfrak{N}}$ ein Normalteiler von $\mathfrak{N}$ mit abelscher p-Faktorgruppe. Falls $\mathfrak{P}_1$ regulär ist, enthält $\mathfrak{G}$ einen Normalteiler $\overline{\mathfrak{G}}$ mit

$$\overline{\mathfrak{G}} \cap \mathfrak{N} = \overline{\mathfrak{N}} \quad \text{und} \quad \mathfrak{G}/\overline{\mathfrak{G}} \simeq \mathfrak{N}/\overline{\mathfrak{N}}.$$

Nehmen wir, um ein Beispiel zu machen, einmal an, daß die in $\mathfrak{P}$ vorhandenen Lösungen der Gleichung $X^p = E$ eine Gruppe $\mathfrak{P}_1$ bilden. Dann ist $\mathfrak{P}_1$ stark abgeschlossen in $\mathfrak{P}$ und regulär. Daher gilt:

Satz 2. *Bilden die in einer Sylowgruppe von $\mathfrak{G}$ vorhandenen Lösungen der Gleichung $X^p = E$ eine Gruppe $\mathfrak{P}_1$, so gibt es zu jedem Normalteiler $\overline{\mathfrak{N}}$ des Normalisators $\mathfrak{N}$ von $\mathfrak{P}_1$ in $\mathfrak{G}$, dessen Faktorgruppe $\mathfrak{N}/\overline{\mathfrak{N}}$ eine abelsche p-Gruppe ist, einen Normalteiler $\overline{\mathfrak{G}}$ von $\mathfrak{G}$ mit $\overline{\mathfrak{G}} \cap \mathfrak{N} = \overline{\mathfrak{N}}$ und $\mathfrak{G}/\overline{\mathfrak{G}} \simeq \mathfrak{N}/\overline{\mathfrak{N}}$.*

Da umgekehrt aus jedem Normalteiler $\overline{\mathfrak{G}}$ von $\mathfrak{G}$ mit abelscher p-Faktorgruppe durch Durchschnittsbildung ein ebensolcher Normalteiler von $\mathfrak{N}$ entspringt, bestätigt sich die in der Einleitung aufgestellte Behauptung, daß die maximalen abelschen p-Faktorgruppen von $\mathfrak{G}$ und $\mathfrak{N}$ isomorph sind. (Übrigens ist das Wort „abelsch“ hierin überflüssig; vgl. Satz 10).

---

[12]) Der letzte Schritt unseres Beweises, der Übergang von zyklischen zu beliebigen abelschen Gruppen, ist überflüssig, wenn man als Faktoren der monomialen Substitutionen an Stelle der Einheitswurzeln die Elemente der Faktorgruppe $\mathfrak{N}/\overline{\mathfrak{N}}$ benutzt. Diese Variante des Burnsideschen Verfahrens ist in letzter Zeit unter dem Namen *Verlagerung* viel benutzt worden. Sie geht auf Schur zurück. Vgl. I. Schur, Neuer Beweis eines Satzes über endliche Gruppen, Sitzungsber. Preuß. Akad. Wiss. 1902, 1013—1019.

(b) $\mathfrak{P}_2 = E$, $\mathfrak{P}_0 = \mathfrak{P}$. Der Hauptsatz besagt: $\mathfrak{P}$ sei eine Sylowgruppe von $\mathfrak{G}$, $\mathfrak{P}_1$ sei schwach abgeschlossen in $\mathfrak{P}$. $\mathfrak{N}$ sei der Normalisator von $\mathfrak{P}_1$, $\overline{\mathfrak{N}}$ ein Normalteiler von $\mathfrak{N}$ mit abelscher p-Faktorgruppe. Falls jedes $P < \mathfrak{P}$ mit jedem $P_1 < \mathfrak{P}_1$ zusammen eine reguläre Gruppe $\{P, P_1\}$ erzeugt, enthält $\mathfrak{G}$ einen Normalteiler $\overline{\mathfrak{G}}$ mit

$$\overline{\mathfrak{G}} \cap \mathfrak{N} = \overline{\mathfrak{N}} \text{ und } \mathfrak{G}/\overline{\mathfrak{G}} \simeq \mathfrak{N}/\overline{\mathfrak{N}}.$$

Die Bedingung, daß alle Gruppen $\{P, P_1\}$ regulär sind, ist z. B. dann erfüllt, wenn $\mathfrak{P}_1$ in dem $(p-1)$-ten Glied $\mathfrak{Z}_{p-1}$ der aufsteigenden Zentrenreihe von $\mathfrak{P}$ enthalten ist ($\mathfrak{Z}_1$ = Zentrum von $\mathfrak{P}$, $\mathfrak{Z}_{i+1}/\mathfrak{Z}_i$ = Zentrum von $\mathfrak{P}/\mathfrak{Z}_i$). Denn wie man leicht erkennt, ist für jedes $i \geqq 1$ die Klasse [13]) der Gruppe $\{P, \mathfrak{Z}_i\}$ **höchstens** i, daher ist die Klasse von $\{P, \mathfrak{P}_1\}$ höchstens $p-1$. Nun ist eine p-Gruppe, deren Klasse **höchstens** $p-1$ ist, regulär [14]). So ergibt sich der

Satz 3. *$\mathfrak{P}$ sei eine p-Sylowgruppe von $\mathfrak{G}$, $\mathfrak{P}_1$ sei schwach abgeschlossen in $\mathfrak{P}$. $\mathfrak{N}$ sei der Normalisator von $\mathfrak{P}_1$ in $\mathfrak{G}$. Wenn $\mathfrak{P}_1$ im $(p-1)$-ten Glied $\mathfrak{Z}_{p-1}$ der aufsteigenden Zentrenreihe von $\mathfrak{P}$ liegt, ist die maximale abelsche p-Faktorgruppe von $\mathfrak{G}$ isomorph zu derjenigen von $\mathfrak{N}$.*

Unter der Voraussetzung $\mathfrak{P}_1 = \mathfrak{Z}_1$ ist dieser Satz schon von Grün bewiesen worden, unter der Voraussetzung $\mathfrak{P}_1 < \mathfrak{Z}_1$ eine schwächere Behauptung von Weisner [15]).

(c) $\mathfrak{P}_0 = \mathfrak{P}_1 = \mathfrak{P}_2$. Der Hauptsatz besagt: $\mathfrak{P}$ sei eine Sylowgruppe von $\mathfrak{G}$, $\mathfrak{P}_1$ sei stark abgeschlossen in $\mathfrak{P}$. $\mathfrak{N}$ sei der Normalisator von $\mathfrak{P}_1$, $\overline{\mathfrak{N}}$ ein Normalteiler von $\mathfrak{N}$ mit abelscher p-Faktorgruppe. Wenn $\mathfrak{P}_1 < \overline{\mathfrak{N}}$ ist, besitzt $\mathfrak{G}$ einen Normalteiler $\overline{\mathfrak{G}}$ mit

$$\overline{\mathfrak{G}} \cap \mathfrak{N} = \overline{\mathfrak{N}} \text{ und } \mathfrak{G}/\overline{\mathfrak{G}} \simeq \mathfrak{N}/\overline{\mathfrak{N}}.$$

Im nächsten Abschnitt wird gezeigt, daß die Einschränkung „$\mathfrak{N}/\overline{\mathfrak{N}}$ abelsch“ unnötig ist (Satz 8). Nehmen wir dies Ergebnis vorweg, so können wir z. B. den folgenden Satz gleich für beliebige Faktorgruppen aussprechen:

Satz 4. *$\mathfrak{P}$ sei eine Sylowgruppe von $\mathfrak{G}$; die in $\mathfrak{P}$ gelegenen Lösungen der Gleichung $X^{p^k} = E$ mögen für eine natürliche Zahl k eine Gruppe $\mathfrak{P}_1$ bilden. $\mathfrak{N}$ sei der Normalisator von $\mathfrak{P}_1$ in $\mathfrak{G}$, $\overline{\mathfrak{N}}$ ein Normalteiler von $\mathfrak{N}$, dessen Index $(\mathfrak{N} : \overline{\mathfrak{N}})$ eine Potenz von p ist. Falls $\mathfrak{P}_1 < \overline{\mathfrak{N}}$ ist, besitzt $\mathfrak{G}$ einen Normalteiler $\overline{\mathfrak{G}}$ mit $\overline{\mathfrak{G}} \cap \mathfrak{N} = \overline{\mathfrak{N}}$ und $\mathfrak{G}/\overline{\mathfrak{G}} \simeq \mathfrak{N}/\overline{\mathfrak{N}}$.*

Hier ist zu erwähnen, daß die in $\mathfrak{P}$ vorhandenen Lösungen der Gleichung $X^{p^k} = E$ sicher dann eine Gruppe bilden, wenn ihre Anzahl nicht durch $p^{k(p-1)}$ teilbar ist [16]), oder wenn sich $\mathfrak{P}$ als Untergruppe eines direkten Produkts von regulären Gruppen darstellen läßt.

(d) $\mathfrak{P}_0 = \mathfrak{P}_1 = \mathfrak{P}$. Der Hauptsatz besagt: $\mathfrak{P}$ sei eine Sylowgruppe von $\mathfrak{G}$, $\mathfrak{N}$ der Normalisator von $\mathfrak{P}$ und $\overline{\mathfrak{N}}$ ein Normalteiler von $\mathfrak{N}$ mit abelscher p-Faktorgruppe. Falls $\mathfrak{P}$ einen Normalteiler $\mathfrak{P}_2$ mit regulärer Faktorgruppe $\mathfrak{P}/\mathfrak{P}_2$ besitzt, derart daß $\overline{\mathfrak{N}}$ die starke Abschließung von $\mathfrak{P}_2$ in $\mathfrak{P}$ enthält, dann besitzt $\mathfrak{G}$ einen Normalteiler $\overline{\mathfrak{G}}$ mit

$$\overline{\mathfrak{G}} \cap \mathfrak{N} = \overline{\mathfrak{N}} \text{ und } \mathfrak{G}/\overline{\mathfrak{G}} \simeq \mathfrak{N}/\overline{\mathfrak{N}}.$$

---

[13]) Unter der Klasse einer p-Gruppe $\mathfrak{H}$ versteht man die Länge der auf- oder absteigenden Zentrenreihe von $\mathfrak{H}$. A. a. O. [4]), 50.

[14]) A. a. O. [4]), Satz 4. 13.

[15]) Grün a. a. O. [3]), Satz 5. Siehe auch L. Weisner, Criteria for the compositeness of finite groups, Duke Math. Journ. **2** (1936), 691—697, Satz 11.

[16]) P. Hall, On a theorem of Frobenius, Proc. London math. Soc. (2) **40** (1936), 468—501, Satz V.

Auch hier ist die Voraussetzung „$\mathfrak{N}/\overline{\mathfrak{N}}$ abelsch" überflüssig (vgl. Satz 10). Wir können daher die folgenden drei Beispiele machen:

Satz 5. *$\mathfrak{P}$ sei eine p-Sylowgruppe von $\mathfrak{G}$, $\mathfrak{N}$ der Normalisator von $\mathfrak{P}$ in $\mathfrak{G}$. Ist $\mathfrak{P}$ regulär, so ist die maximale p-Faktorgruppe von $\mathfrak{G}$ isomorph zu derjenigen von $\mathfrak{N}$.*

Zum Beweis hat man nur $\mathfrak{P}_2 = E$ zu setzen.

Als handlichste von allen Folgerungen aus dem Hauptsatz erwähnen wir den nachstehenden Spezialfall von (5):

Satz 6. *Ist die Ordnung von $\mathfrak{G}$ nicht durch p^{p+1} teilbar, so ist die maximale p-Faktorgruppe von $\mathfrak{G}$ isomorph zu derjenigen des Normalisators einer p-Sylowgruppe von $\mathfrak{G}$.*

Beweis. Eine p-Gruppe, deren Ordnung $< p^{p+1}$ ist, ist regulär[17]).

Zum Schluß ein Beispiel mit $\mathfrak{P}_2 \neq E$. Wir bezeichnen dabei, wenn $\mathfrak{H}$ eine beliebige endliche Gruppe und c eine natürliche Zahl ist, mit $\mathfrak{H}^c$ den kleinsten Normalteiler von $\mathfrak{H}$, für welchen $\mathfrak{H}/\mathfrak{H}^c$ eine p-Gruppe der Klasse $\leqq c$ ist.

Satz 7. *$\mathfrak{P}$ sei eine p-Sylowgruppe von $\mathfrak{G}$, $\mathfrak{N}$ der Normalisator von $\mathfrak{P}$ in $\mathfrak{G}$. Falls $c \leqq p-1$ ist, gilt*

$$\mathfrak{G}^c \cap \mathfrak{N} = \mathfrak{N}^c(\mathfrak{P}^{p-1})^*.$$

Dabei bedeutet $(\mathfrak{P}^{p-1})^*$ die starke Abschließung von $\mathfrak{P}^{p-1}$ in $\mathfrak{P}$.

Beweis. Die Beziehung

$$\mathfrak{N}^c(\mathfrak{P}^{p-1})^* < \mathfrak{G}^c \cap \mathfrak{N}$$

ist trivial. Denn $\mathfrak{G}^c \cap \mathfrak{N}$ ist ein Normalteiler von $\mathfrak{N}$, dessen Faktorgruppe eine p-Gruppe der Klasse $\leqq c$ ist, also ist zunächst einmal $\mathfrak{N}^c < \mathfrak{G}^c \cap \mathfrak{N}$. Ferner ist $\mathfrak{G}^c \cap \mathfrak{P}$ ein Normalteiler von $\mathfrak{P}$, dessen Faktorgruppe höchstens die Klasse $c \leqq p-1$ hat, also ist $\mathfrak{P}^{p-1} < \mathfrak{G}^c \cap \mathfrak{P}$ und damit auch $(\mathfrak{P}^{p-1})^* < \mathfrak{G}^c \cap \mathfrak{P}$.

Die umgekehrte Beziehung

$$\mathfrak{G}^c \cap \mathfrak{N} < \mathfrak{N}^c(\mathfrak{P}^{p-1})^*$$

folgt aus dem betrachteten Spezialfall des Hauptsatzes: Mit $\overline{\mathfrak{N}} = \mathfrak{N}^c(\mathfrak{P}^{p-1})^*$ und $\mathfrak{P}_2 = \mathfrak{P}^{p-1}$ sind seine Voraussetzungen erfüllt, also besitzt $\mathfrak{G}$ einen Normalteiler $\overline{\mathfrak{G}}$ mit $\overline{\mathfrak{G}} \cap \mathfrak{N} = \overline{\mathfrak{N}}$ und $\mathfrak{G}/\overline{\mathfrak{G}} \simeq \mathfrak{N}/\overline{\mathfrak{N}}$. Diese Isomorphiebeziehung zeigt, daß $\mathfrak{G}/\overline{\mathfrak{G}}$ eine p-Gruppe höchstens der Klasse c ist, daß also $\mathfrak{G}^c < \overline{\mathfrak{G}}$ ist. Nun zeigt die Durchschnittsbeziehung, daß $\mathfrak{G}^c \cap \mathfrak{N} < \overline{\mathfrak{N}}$ ist, was zu beweisen war.

Aus Satz 7 folgt, daß $(\mathfrak{N}^c \cap \mathfrak{P})(\mathfrak{P}^{p-1})^*$, als Durchschnitt des Normalteilers $\mathfrak{G}^c$ mit $\mathfrak{P}$, eine Sylowgruppe von $\mathfrak{G}^c$ ist[18]). — Der Spezialfall $c = 1$ von Satz 7 ist von Grün in der etwas schwächeren Fassung $\mathfrak{G}^1 \cap \mathfrak{N} = \mathfrak{N}^1(\mathfrak{P}^1)^*$ bewiesen worden[19]). Für $c = p$ gilt Satz 7 nicht mehr; das zeigt das Beispiel in Abschnitt V.

IV. Beliebige p-Faktorgruppen.

Durch einfache Induktionsschlüsse in bezug auf die Ordnung von $\mathfrak{G}$ folgen aus dem Hauptsatz zwei Sätze (8 und 10), durch die auch nichtabelsche p-Faktorgruppen zugänglich werden. Anwendungen dieser beiden Sätze sind schon im vorigen Abschnitt erwähnt worden.

---

[17]) A. a. O. [4]), Satz 4. 14.

[18]) Vgl. z. B. H. Zassenhaus, Lehrbuch der Gruppentheorie 1 (Leipzig und Berlin 1937), S. 100, Satz 2.

[19]) A. a. O. [3]), Satz 9.

Satz 8. *Der Hauptsatz (Satz 1) bleibt richtig, wenn in ihm die Voraussetzung „$\mathfrak{N}/\overline{\mathfrak{N}}$ abelsch" durch die schwächere „$\mathfrak{P}_1\overline{\mathfrak{N}}/\overline{\mathfrak{N}}$ abelsch" ersetzt wird.*

Beweis. Ist $\mathfrak{P}_1\overline{\mathfrak{N}} = \mathfrak{N}$, so ist $\mathfrak{N}/\overline{\mathfrak{N}}$ abelsch, und wir haben nichts zu beweisen. Ist $\mathfrak{P}_1\overline{\mathfrak{N}} \neq \mathfrak{N}$, so gibt es einen Normalteiler $\mathfrak{N}'$ von $\mathfrak{N}$, der $\mathfrak{P}_1$ und $\overline{\mathfrak{N}}$ enthält und den Index $(\mathfrak{N}:\mathfrak{N}') = p$ hat. Mit $\mathfrak{N}'$ statt $\overline{\mathfrak{N}}$ sind die Voraussetzungen des Hauptsatzes erfüllt. Also gibt es einen Normalteiler $\mathfrak{G}'$ von $\mathfrak{G}$ mit dem Index p, für welchen $\mathfrak{G}' \cap \mathfrak{N} = \mathfrak{N}'$ ist. Nun erfüllen, wie man ohne weiteres sieht, die Gruppen

$$\mathfrak{G}',\ \mathfrak{P}' = \mathfrak{G}' \cap \mathfrak{P},\ \mathfrak{P}_0' = \mathfrak{G}' \cap \mathfrak{P}_0,\ \mathfrak{P}_1,\ \mathfrak{P}_2,\ \mathfrak{N}',\ \overline{\mathfrak{N}}$$

die Voraussetzungen von Satz 8. Nehmen wir diesen für die kleinere Gruppe $\mathfrak{G}'$ schon als richtig an, so besitzt $\mathfrak{G}'$ einen Normalteiler $\overline{\mathfrak{G}}$ mit $\overline{\mathfrak{G}} \cap \mathfrak{N}' = \overline{\mathfrak{N}}$ und $(\mathfrak{G}':\overline{\mathfrak{G}}) = (\mathfrak{N}':\overline{\mathfrak{N}})$.

Wir behaupten:

(a) $\overline{\mathfrak{G}}$ ist ein Normalteiler von $\mathfrak{G}$. Da $\mathfrak{G}'\mathfrak{N} = \mathfrak{G}$ ist, genügt es zu zeigen, daß $\overline{\mathfrak{G}}^N = \overline{\mathfrak{G}}$ ist für jedes $N < \mathfrak{N}$. Wäre dies nicht der Fall, so wäre der Durchschnitt $\mathfrak{D} = \overline{\mathfrak{G}}^N \cap \overline{\mathfrak{G}}$, ebenso wie $\overline{\mathfrak{G}}$ und $\overline{\mathfrak{G}}^N$, ein Normalteiler von $\mathfrak{G}'$, dessen Index eine Potenz von p ist, und zwar wäre $(\mathfrak{G}':\mathfrak{D}) > (\mathfrak{G}':\overline{\mathfrak{G}})$. D. h. die Ordnung von $\mathfrak{D}$ wäre durch eine kleinere Potenz von p teilbar als die Ordnung von $\overline{\mathfrak{G}}$. Anderseits ist $\overline{\mathfrak{N}} < \mathfrak{D}$, und $\overline{\mathfrak{N}}$ enthält eine p-Sylowgruppe von $\overline{\mathfrak{G}}$.

(b) Es ist $\overline{\mathfrak{G}} \cap \mathfrak{N} = \overline{\mathfrak{N}}$. Denn es ist

$$\overline{\mathfrak{G}} \cap \mathfrak{N} = \overline{\mathfrak{G}} \cap \mathfrak{G}' \cap \mathfrak{N} = \overline{\mathfrak{G}} \cap \mathfrak{N}' = \overline{\mathfrak{N}}.$$

(c) Es ist $\overline{\mathfrak{G}}\mathfrak{N} = \mathfrak{G}$. Denn $(\mathfrak{G}:\overline{\mathfrak{G}})$ ist eine Potenz von p, und $\mathfrak{N}$ enthält $\mathfrak{P}$.

Damit ist Satz 8 bewiesen.

Die Voraussetzung „$\mathfrak{P}_1\overline{\mathfrak{N}}/\overline{\mathfrak{N}}$ abelsch" besagt, daß die Kommutatorgruppe von $\mathfrak{P}_1$ in $\overline{\mathfrak{N}}$ enthalten ist, und ist jedenfalls erfüllt, wenn $\mathfrak{P}_1 < \overline{\mathfrak{N}}$ ist. Von dieser Art war das Beispiel, das Satz 4 des vorigen Abschnitts gibt. Eine weitere Folgerung soll hier erwähnt werden:

Satz 9. *$\mathfrak{P}_1$ sei eine Untergruppe der p-Sylowgruppe $\mathfrak{P}$ von $\mathfrak{G}$. Notwendig und hinreichend dafür, daß es einen Normalteiler $\overline{\mathfrak{G}}$ von $\mathfrak{G}$ gibt, dessen Index $(\mathfrak{G}:\overline{\mathfrak{G}}) = p^\alpha$ ist und der $\mathfrak{P}_1$ als Sylowgruppe enthält, ist die Bedingung: $\mathfrak{P}_1$ ist stark abgeschlossen in $\mathfrak{P}$, und der Normalisator $\mathfrak{N}$ von $\mathfrak{P}_1$ in $\mathfrak{G}$ besitzt einen Normalteiler $\overline{\mathfrak{N}}$ mit dem Index $(\mathfrak{N}:\overline{\mathfrak{N}}) = p^\alpha$, der $\mathfrak{P}_1$ als Sylowgruppe enthält.*

Beweis. Die Bedingung ist notwendig: Als Durchschnitt von $\mathfrak{P}$ mit dem Normalteiler $\overline{\mathfrak{G}}$ von $\mathfrak{G}$ muß $\mathfrak{P}_1$ in $\mathfrak{P}$ stark abgeschlossen sein. Setzen wir ferner $\overline{\mathfrak{G}} \cap \mathfrak{N} = \overline{\mathfrak{N}}$, so ist $\mathfrak{P}_1$ Sylowgruppe von $\overline{\mathfrak{N}}$, und es ist $(\mathfrak{N}:\overline{\mathfrak{N}}) = (\mathfrak{G}:\overline{\mathfrak{G}}) = p^\alpha$.

Die Bedingung ist hinreichend: Nach Satz 8, angewandt auf $\mathfrak{G}, \mathfrak{P}, \mathfrak{P}_0 = \mathfrak{P}_2 = \mathfrak{P}_1, \mathfrak{N}, \overline{\mathfrak{N}}$ gibt es in $\mathfrak{G}$ einen Normalteiler $\overline{\mathfrak{G}}$ mit $\overline{\mathfrak{G}} \cap \mathfrak{N} = \overline{\mathfrak{N}}$ und $\mathfrak{G}/\overline{\mathfrak{G}} \simeq \mathfrak{N}/\overline{\mathfrak{N}}$. Aus der ersten Tatsache folgt $\overline{\mathfrak{G}} \cap \mathfrak{P} = \mathfrak{P}_1$, also ist $\mathfrak{P}_1$ eine Sylowgruppe von $\overline{\mathfrak{G}}$. Aus der zweiten folgt $(\mathfrak{G}:\overline{\mathfrak{G}}) = (\mathfrak{N}:\overline{\mathfrak{N}}) = p^\alpha$.

Die hinreichende Bedingung könnte natürlich noch abgeschwächt werden, weil Satz 8 nicht voll ausgenützt wurde.

Wenngleich Satz 8 sehr umfassend ist, ist in ihm der Satz 5 über die regulären Sylowgruppen nicht unmittelbar enthalten. Das leistet erst der folgende

Satz 10. *Der Hauptsatz (Satz 1) bleibt richtig, wenn in ihm die Voraussetzung „$\mathfrak{N}/\overline{\mathfrak{N}}$ abelsch" gestrichen und dafür die Voraussetzung „$\mathfrak{P}_1$ stark abgeschlossen in $\mathfrak{P}$" hinzugefügt wird.*

Beweis. Wir nehmen den Satz für kleinere Gruppen als $\mathfrak{G}$ für bewiesen an und unterscheiden die zwei Fälle, ob $\mathfrak{P}_1\overline{\mathfrak{N}} \neq \mathfrak{N}$ oder $= \mathfrak{N}$ ist.

Es sei $\mathfrak{P}_1\overline{\mathfrak{N}} = \mathfrak{N}' \neq \mathfrak{N}$. Da $\mathfrak{N}'$ ein Normalteiler von $\mathfrak{N}$ ist, dessen Index $(\mathfrak{N} : \mathfrak{N}')$ eine Potenz von p ist und der $\mathfrak{P}_1$ enthält, liegt für $\mathfrak{N}'$ (statt $\overline{\mathfrak{N}}$) der Fall von Satz 8 vor. Daher gibt es einen echten Normalteiler $\mathfrak{G}'$ von $\mathfrak{G}$ mit $\mathfrak{G}' \cap \mathfrak{N} = \mathfrak{N}'$ und $(\mathfrak{G} : \mathfrak{G}') = (\mathfrak{N} : \mathfrak{N}')$. Für $\mathfrak{G}'$ ist Satz 10 nach Induktionsannahme schon richtig. Wir wenden ihn auf die Gruppen

$$\mathfrak{P}' = \mathfrak{P} \cap \mathfrak{G}',\ \mathfrak{P}_0' = \mathfrak{P}_0 \cap \mathfrak{G}',\ \mathfrak{P}_1,\ \mathfrak{P}_2,\ \mathfrak{N}',\ \overline{\mathfrak{N}}$$

an, welche die Voraussetzungen offenbar erfüllen. Es ergibt sich ein Normalteiler $\overline{\mathfrak{G}}$ von $\mathfrak{G}'$ mit $\overline{\mathfrak{G}} \cap \mathfrak{N}' = \overline{\mathfrak{N}}$ und $(\mathfrak{G}' : \overline{\mathfrak{G}}) = (\mathfrak{N}' : \overline{\mathfrak{N}})$. Wie beim Beweis von Satz 8, Punkt **(a)**—**(c)**, ergibt sich, daß $\overline{\mathfrak{G}}$ ein Normalteiler von $\mathfrak{G}$ mit den Eigenschaften $\overline{\mathfrak{G}} \cap \mathfrak{N} = \overline{\mathfrak{N}}$ und $\overline{\mathfrak{G}}\mathfrak{N} = \mathfrak{G}$ ist.

Es sei nun $\mathfrak{P}_1\mathfrak{N} = \mathfrak{N}$. Da der Fall einer zyklischen Faktorgruppe $\mathfrak{N}/\overline{\mathfrak{N}}$ schon durch den Hauptsatz erledigt ist, können wir im folgenden voraussetzen, daß $\mathfrak{N}/\overline{\mathfrak{N}}$ nicht zyklisch ist. Dann enthält $\mathfrak{N}$ mindestens zwei verschiedene Normalteiler $\mathfrak{A}', \mathfrak{A}''$ vom Index p, die ihrerseits $\overline{\mathfrak{N}}$ enthalten. Wir setzen $\mathfrak{A}' \cap \mathfrak{P}_1 = \mathfrak{P}_1'$ und $\mathfrak{A}'' \cap \mathfrak{P}_1 = \mathfrak{P}_1''$. Wegen $\mathfrak{P}_1\overline{\mathfrak{N}} = \mathfrak{N}$ sind $\mathfrak{P}_1'$ und $\mathfrak{P}_1''$ zwei verschiedene Normalteiler des Index p in $\mathfrak{P}_1$, erzeugen also zusammen $\mathfrak{P}_1$. Falls daher sowohl $\mathfrak{P}_1'$ wie $\mathfrak{P}_1''$ in $\mathfrak{G}$ invariant ist, ist $\mathfrak{G} = \mathfrak{N}$, und es ist nichts zu beweisen. Wir beschränken uns weiter auf den Fall, daß $\mathfrak{P}_1'$ nicht in $\mathfrak{G}$ invariant ist. Der Normalisator $\mathfrak{H}$ von $\mathfrak{P}_1'$ in $\mathfrak{G}$ ist also eine echte Untergruppe von $\mathfrak{G}$. Wir behaupten der Reihe nach:

(a) $\mathfrak{H}$ enthält einen Normalteiler $\overline{\mathfrak{H}}$ mit $\overline{\mathfrak{H}} \cap \mathfrak{N} = \overline{\mathfrak{N}}$, dessen Index $(\mathfrak{H} : \overline{\mathfrak{H}})$ eine Potenz von p ist.

Beweis. $\mathfrak{N}$ liegt in $\mathfrak{H}$, weil $\mathfrak{P}_1'$ als Durchschnitt der beiden Normalteiler $\mathfrak{P}_1$ und $\mathfrak{A}'$ von $\mathfrak{N}$ selbst ein Normalteiler von $\mathfrak{N}$ ist. Nun ergibt sich die Behauptung, wenn man Satz 10 auf $\mathfrak{H}$ statt $\mathfrak{G}$ anwendet. Daß die Voraussetzungen erfüllt sind, sieht man ohne weiteres.

(b) $\mathfrak{G}$ enthält einen Normalteiler $\mathfrak{G}'$ mit $\mathfrak{G}' \cap \mathfrak{N} = \mathfrak{A}'$ und dem Index $(\mathfrak{G} : \mathfrak{G}') = p$.

Beweis. Mit $\mathfrak{A}'$ statt $\overline{\mathfrak{N}}$ sind die Voraussetzungen des Hauptsatzes erfüllt.

Wir bezeichnen den Normalisator von $\mathfrak{P}_1'$ in $\mathfrak{G}'$ mit $\mathfrak{N}'$; es ist $\overline{\mathfrak{N}} < \mathfrak{N}'$. Es gilt:

(c) $\mathfrak{N}'$ enthält einen Normalteiler $\overline{\mathfrak{N}'}$ mit $\overline{\mathfrak{N}'} \cap \mathfrak{N} = \overline{\mathfrak{N}}$, dessen Index $(\mathfrak{N}' : \overline{\mathfrak{N}'})$ eine Potenz von p ist.

Beweis. Wir setzen $\overline{\mathfrak{N}'} = \overline{\mathfrak{H}} \cap \mathfrak{N}'$. Es wird

$$\overline{\mathfrak{N}'} \cap \mathfrak{N} = \mathfrak{N}' \cap \overline{\mathfrak{H}} \cap \mathfrak{N} = \mathfrak{N}' \cap \overline{\mathfrak{N}} = \overline{\mathfrak{N}}.$$

Ferner ist $(\mathfrak{N}' : \overline{\mathfrak{N}}) = (\mathfrak{N}'\overline{\mathfrak{H}} : \overline{\mathfrak{H}})$, und der letztere Index ist als Teiler von $(\mathfrak{H} : \overline{\mathfrak{H}})$ eine Potenz von p.

(d) $\mathfrak{G}'$ enthält einen Normalteiler $\overline{\mathfrak{G}}$ mit $\overline{\mathfrak{G}} \cap \mathfrak{N}' = \overline{\mathfrak{N}'}$, dessen Index $(\mathfrak{G}' : \overline{\mathfrak{G}})$ eine Potenz von p ist.

Beweis. Wir setzen $\mathfrak{P} \cap \mathfrak{G}' = \mathfrak{P}'$, $\mathfrak{P}_i \cap \mathfrak{G}' = \mathfrak{P}_i'$ $(i = 0, 2)$ und zeigen, daß die Gruppen $\mathfrak{G}', \mathfrak{P}', \mathfrak{P}_0', \mathfrak{P}_1', \mathfrak{P}_2', \mathfrak{N}', \overline{\mathfrak{N}'}$ die Voraussetzungen des Satzes 10 erfüllen: $\mathfrak{P}'$ ist Sylowgruppe von $\mathfrak{G}'$. $\mathfrak{P}_k'$ $(k = 0, 1)$ ist, als Durchschnitt von $\mathfrak{G}'$ mit der stark abgeschlossenen Gruppe $\mathfrak{P}_k$, stark abgeschlossen sogar in $\mathfrak{P}$. $\mathfrak{N}'$ ist nach Definition der Normalisator von $\mathfrak{P}_1'$ in $\mathfrak{G}'$. $\overline{\mathfrak{N}'}$ ist nach **(c)** ein Normalteiler von $\mathfrak{N}'$, dessen Index $(\mathfrak{N}' : \overline{\mathfrak{N}'})$ eine

Potenz von p ist. $\mathfrak{P}_2'$ ist sogar ein Normalteiler von $\mathfrak{P}_0$, erst recht von $\mathfrak{P}_0'$. Für $P_k' < \mathfrak{P}_k'$ ist

$$\{P_0', P_1', \mathfrak{P}_2'\}/\mathfrak{P}_2' \simeq \{P_0', P_1', \mathfrak{P}_2\}/\mathfrak{P}_2,$$

und besitzt somit die Eigenschaft R. Die starke Abschließung von $\mathfrak{P}_2'$ in $\mathfrak{P}'$ bezüglich $\mathfrak{G}'$ liegt, als Untergruppe der starken Abschließung von $\mathfrak{P}_2$ in $\mathfrak{P}$ bezüglich $\mathfrak{G}$, nach Voraussetzung in $\overline{\mathfrak{N}}$, daher nach **(c)** erst recht in $\overline{\mathfrak{N}'}$. Damit haben wir alle Voraussetzungen nachgeprüft; Satz 10, auf $\mathfrak{G}'$ angewendet, liefert die Behauptung **(d)**.

Daß $\overline{\mathfrak{G}}$ die in Satz 10 ausgesprochenen Eigenschaften hat, sieht man wieder wie beim Beweis von Satz 8, wenn man die Beziehung $\overline{\mathfrak{G}} \cap \mathfrak{N} < \mathfrak{N}'$ beachtet.

V. Ein Gegenbeispiel.

Wir bilden jetzt das in der Einleitung erwähnte Beispiel einer Gruppe $\mathfrak{G}$, die keinen Normalteiler vom Index p, wohl aber eine Sylowgruppe $\mathfrak{P}$ der Ordnung p^{p+1} enthält, deren Normalisator einen Normalteiler vom Index p besitzt.

Es sei zuerst $p > 2$. Wir wählen für $\mathfrak{G}$ die Gruppe derjenigen monomialen Substitutionen A von $p+1$ Variablen $x_0, x_1, \ldots, x_p$, deren Faktoren p-te Einheitswurzeln mit dem Produkt $\Delta(A) = 1$ sind. Die Ordnung von $\mathfrak{G}$ ist $(p+1)!\, p^p$. Eine Sylowgruppe $\mathfrak{P}$ besteht z. B. aus den Substitutionen $\begin{pmatrix} x_0 & x_\nu \\ \varepsilon_0 x_0 & \varepsilon_\nu x_{\nu+k} \end{pmatrix}$, wobei ν und $\nu+k$ die Werte $1, 2, \ldots, p$ durchlaufen und $\nu + k$ mod p zu reduzieren ist. Bei $\mathfrak{P}$ bleibt x_0 fest und wird mit allen p-ten Einheitswurzeln versehen. Da $\mathfrak{P}$ nur diesen einen transitiven Konstituenten des Grades 1 hat, muß x_0 auch bei dem Normalisator $\mathfrak{N}$ von $\mathfrak{P}$ fest sein und wird natürlich von $\mathfrak{N}$ erst recht mit allen p-ten Einheitswurzeln versehen. Daher bilden diejenigen Substitutionen aus $\mathfrak{N}$, die x_0 mit dem Faktor 1 versehen, einen Normalteiler $\overline{\mathfrak{N}}$ mit dem Index p.

Anderseits besitzt $\mathfrak{G}$ keinen Normalteiler $\overline{\mathfrak{G}}$ vom Index p. Denn ein solcher müßte mindestens eine von E verschiedene Diagonalsubstitution D enthalten. Wegen $\Delta(D) = 1$ stimmen die Diagonalfaktoren von D nicht sämtlich überein. Daher kann man aus D durch Kommutatorbildung mit geeigneten Transpositionen, durch Ähnlichkeitstransformationen und durch Bilden von Produkten den vollen Normalteiler $\mathfrak{D}$ aller Diagonalsubstitutionen von $\mathfrak{G}$ erzeugen. Es wäre also $\mathfrak{D} < \overline{\mathfrak{G}}$. Das würde besagen: $\mathfrak{G}/\mathfrak{D}$ besitzt einen Normalteiler $\overline{\mathfrak{G}}/\mathfrak{D}$ vom Index p. Das widerspricht der Tatsache, daß $\mathfrak{G}/\mathfrak{D}$ zur Gruppe aller Permutationen von $x_0, x_1, \ldots, x_p$ isomorph ist, welche keinen Normalteiler vom Index p enthält.

Im Fall $p = 2$ geht es noch einfacher; wir können für $\mathfrak{G}$ die alternierende Gruppe des Grades 6 wählen.

VI. Schlußbemerkungen.

Wir haben uns auf die Behandlung der Frage beschränkt, wann man aus der Existenz einer p-Faktorgruppe gewisser Untergruppen auf die Existenz einer isomorphen Faktorgruppe der ganzen Gruppe $\mathfrak{G}$ schließen kann. Nun besteht eine Hauptanwendung der Methode der monomialen Darstellung darin, daß aus möglichst schwachen Voraussetzungen die Existenz irgendeiner Faktorgruppe der Ordnung p von $\mathfrak{G}$ erschlossen wird, z. B. zu dem Zweck, die Nichteinfachheit von $\mathfrak{G}$ nachzuweisen. Wir bemerken, daß sich aus dem Beweis des Hauptsatzes auch leicht Sätze dieser Art ergeben. Daß $\mathfrak{G}$ eine Faktorgruppe der Ordnung p besitzt, kann man unter geeigneten Voraussetzungen schon dann folgern, wenn man den Punkt **(d)** des Beweises des Hauptsatzes hat. Punkt **(d)** besagt,

daß für ein Element $P_0 < \mathfrak{P}_0$, dessen Diagonalfaktoren p-te Einheitswurzeln sind, das Produkt der Diagonalfaktoren gleich dem Faktor ε_1 von x_1 ist. Nun kann man $\varepsilon_1 \neq 1$ erzwingen durch die Voraussetzung, daß P_0 nicht in $\overline{\mathfrak{N}}$ liegt, und man kann erzwingen, daß für jeden Zyklus Z von P_0, dessen Grad > 1 ist, $\Delta(Z) = 1$ wird, indem man voraussetzt, daß $P_0^p < \mathfrak{P}_2$ liegt. Bis zum Beweis des Punktes **(d)** einschließlich wurde die einschneidendste Voraussetzung des Hauptsatzes, daß $\mathfrak{P}_0$ in $\mathfrak{P}$ stark abgeschlossen ist, gar nicht benutzt, wie seinerzeit ausdrücklich hervorgehoben wurde. So erhält man den Satz:

Satz 11. *$\mathfrak{P}$ sei eine p-Sylowgruppe von $\mathfrak{G}$, $\mathfrak{P}_1$ sei in $\mathfrak{P}$ schwach abgeschlossen. $\mathfrak{N}$ sei der Normalisator von $\mathfrak{P}_1$ in $\mathfrak{G}$ und $\overline{\mathfrak{N}}$ ein Normalteiler von $\mathfrak{N}$ mit abelscher p-Faktorgruppe $\mathfrak{N}/\overline{\mathfrak{N}}$. P_0 sei ein Element von $\mathfrak{P}$, welches nicht in $\overline{\mathfrak{N}}$ liegt.*

$\mathfrak{G}$ besitzt einen P_0 nicht enthaltenden Normalteiler $\overline{\mathfrak{G}}$ vom Index p, falls es in $\mathfrak{P}$ eine Untergruppe $\mathfrak{P}_2$ mit den folgenden Eigenschaften gibt:

$P_0^p < \mathfrak{P}_2$,

$\mathfrak{P}_2$ ist ein Normalteiler von $\{P_0, \mathfrak{P}_1, \mathfrak{P}_2\}$,

die Faktorgruppe $\{P_0, P_1, \mathfrak{P}_2\}/\mathfrak{P}_2$ hat die Eigenschaft R für jedes Element $P_1 < \mathfrak{P}_1$,

die starke Abschließung von $\mathfrak{P}_2$ in $\mathfrak{P}$ liegt in $\overline{\mathfrak{N}}$.

Ähnlich wie dies vom Hauptsatz in Abschnitt III gezeigt wurde, läßt sich auch Satz 11 auf verschiedene Arten anwenden. Es werde nur ein Beispiel angeführt, bei dem $\mathfrak{P}_2 = E$ ist:

Satz 12. *$\mathfrak{P}$ sei eine p-Sylowgruppe von $\mathfrak{G}$, $\mathfrak{P}_1$ sei in $\mathfrak{P}$ schwach abgeschlossen. $\mathfrak{N}$ sei der Normalisator von $\mathfrak{P}_1$ in $\mathfrak{G}$ und $\overline{\mathfrak{N}}$ die Kommutatorgruppe von $\mathfrak{N}$. Falls es in $\mathfrak{P}$ ein Element P_0 der Ordnung p gibt, welches nicht in $\overline{\mathfrak{N}}$ liegt, wohl aber mit jedem Element von $\mathfrak{P}_1$ zusammen eine Gruppe der Klasse $\leqq p-1$ erzeugt, so enthält $\mathfrak{G}$ einen Normalteiler $\overline{\mathfrak{G}}$ vom Index p, der P_0 nicht enthält.*

Mit der stärkeren Voraussetzung, daß P_0 mit jedem Element von $\mathfrak{P}_1$ vertauschbar sein soll, hat Zappa[20]) kürzlich diesen Satz veröffentlicht.

---

[20]) A. a. O. [10]), 174.

Eingegangen 10. Mai 1939.

On groups of automorphisms.

By *P. Hall* in Cambridge (England).

1. The present paper is a contribution to the elementary arithmetic of groups. It is primarily concerned with a certain class of summation formulae involving the orders of groups of automorphisms. The main interest probably lies in the interpretation of these formulae in terms of the notion, here introduced, of a *pure situation* and its various possible *realizations*.

2. Let $t(G)$ be the order of the group of automorphisms $T(G)$ of the group G, and let $n(G)$ be an arithmetical function depending on G. Then the formulae in question have the following form:

$$\sum_{G \in \mathfrak{S}} \frac{n(G)}{t(G)} = f(n; \mathfrak{S}), \tag{1}$$

the sum being taken over all groups G of a certain system $\mathfrak{S}$, where $f(n; \mathfrak{S})$ is intended to denote an expression depending only on the function n and the system $\mathfrak{S}$, but not involving explicitly the properties of the individual groups G.

Some examples will make the nature of the formulae clear. Let us assume first, for simplicity, that our system consists of all $\omega(k)$ Abelian groups of order 2^k, where $\omega(k)$ is the number of unrestricted partitions of the integer k. This system will be denoted by $\mathfrak{S}_k$. And let us choose for our arithmetical function the number of composition series of G, a number we denote by $v = v(G)$. Then we have

$$f(v; \mathfrak{S}_k) = 1, \tag{2}$$

and

$$f(v^2; \mathfrak{S}_k) = k!. \tag{3}$$

Next, let $n_h(G)$ be the number of subgroups of order 2^h in G, where $0 \leqq h \leqq k$. Then

$$f(vn_h; \mathfrak{S}_k) = \binom{k}{h}. \tag{4}$$

In particular, if $d(G)$ is the number of independent generators of G,

$$f(2^d v; \mathfrak{S}_k) = k + 1. \tag{5}$$

A more general result may be described as follows. Let $k_1, k_2, \ldots, k_r$ be any ordered set of positive integers with sum equal to k. With this set are associated certain chains of subgroups of G, viz. all chains of the form

$$G = G_0 > G_1 > G_2 > \cdots > G_r = 1,$$

where G_{i-1}/G_i is of order precisely 2^{ki}. The total number of such chains in a group G of $\mathfrak{S}_k$ will be denoted by $v_{k_1, k_2, \ldots, k_r}(G)$. It is to be observed that as a result of the duality properties of Abelian groups, this function is independent of the order of the r numbers k_i. We then have

$$f(vv_{k_1,k_2,\ldots,k_r}; \mathfrak{S}_k) = \frac{k!}{k_1!\, k_2! \cdots k_r!}. \tag{6}$$

Since $v_{1,1,\ldots,1} = v$, it is clear that (3) is a particular case of (6). So also is (2), for $v_k = 1$. And again (4), for $v_{k-h,h} = n_h$.

In all these results, the function n in $f(n; \mathfrak{S}_k)$ is a multiple of the number of composition series v. There is a corresponding set of formulae in which v is replaced by 1. These are most easily expressible in terms of the quantity [1])

$$\sigma_k = f(1; \mathfrak{S}_k) = \frac{2^{\frac{1}{2}k(k-1)}}{(2^k-1)(2^{k-1}-1)\cdots(2-1)}. \tag{7}$$

In fact, we have

$$f(v_{k_1,k_2,\ldots,k_r}; \mathfrak{S}_k) = \sigma_{k_1}\sigma_{k_2}\cdots\sigma_{k_r}. \tag{8}$$

In particular,

$$f(n_k; \mathfrak{S}_k) = \sigma_{k-h}\,\sigma_h. \tag{9}$$

3. To proceed further, we must introduce functions which reveal the structure of individual groups in closer detail. Since it is just as easy to do so, we shall now take instead of $\mathfrak{S}_k$ the system of all Abelian groups of order m. This system will be denoted by $\mathfrak{S}^m$. Here, m is any positive integer.

Let $Q_1, Q_2, \ldots, Q_r$ be any ordered set of abstract Abelian groups, not necessarily distinct, but subject to the condition that the product of their orders is equal to m. With this set are associated certain chains of subgroups of the groups G of our system $\mathfrak{S}^m$, viz. all chains of the form

$$G = G_0 > G_1 > G_2 > \cdots > G_r = 1$$

for which

$$G_{i-1}/G_i \simeq Q_i \qquad (i = 1, 2, \ldots, r).$$

The total number of such chains in G, which may be zero, will be denoted by $v_{Q_1,Q_2,\ldots,Q_r}(G)$. This function is independent of the order of the suffixes Q_i, and we have the key result

$$f(v_{Q_1,Q_2,\ldots,Q_r}; \mathfrak{S}^m) = \frac{1}{t(Q_1)\,t(Q_2)\cdots t(Q_r)}. \tag{10}$$

With the help of (7), we can easily deduce from this the formulae given above for the special case $m = 2^k$. For example, in this case, obviously

$$v_{k_1,k_2,\ldots,k_r} = \sum_{(Q)} v_{Q_1,Q_2,\ldots,Q_r},$$

where, in the summation on the right, each Q_i is to run independently through the $\omega(k_i)$ distinct Abelian groups of order 2^{ki}. Thus, by performing this summation over the formulae (10), and using (7), we obtain (8).

We may express this position by saying that (10) is a *primary* formula, from which the *secondary* formula (8) is obtainable by summation. This distinction of primary and secondary formulae is of course purely relative.

4. We shall now give, as a specimen, a proof of the simplest of our primary formulae, viz. (2).

---

[1]) For a proof of (7), see *P. Hall*, "A partition formula connected with Abelian groups", Comment. Math. Helvet. **11** (1938), 126.

Let G be any group of $\mathfrak{S}_k$, and let

$$G = G_0 > G_1 > \cdots > G_k = 1$$

be any one of the $v(G)$ distinct composition series of G. Let us choose from each of the k sets $G_{i-1} - G_i$ $(i = 1, 2, \ldots, k)$ an arbitrary element ξ_i. Clearly, the k elements $\xi_1, \xi_2, \ldots, \xi_k$ will generate G; or, as we may also express it, they form a *k-basis* of G. Moreover, in terms of the ξ's, the defining relations of G take the form

$$(11) \qquad \begin{cases} \xi_i^2 = \varphi_i(\xi_{i+1}, \ldots, \xi_k) & (i = 1, 2, \ldots, k-1), \\ \xi_k^2 = 1, \quad \xi_i^{-1}\xi_j^{-1}\xi_i\xi_j = 1 & (i, j = 1, 2, \ldots, k). \end{cases}$$

Conversely, if $\xi_1, \ldots, \xi_k$ is a k-basis of G for which the defining relations of G may be expressed in the form (11), then the subgroups $G_i = \{\xi_{i+1}, \ldots, \xi_k\}$ clearly form a composition series of G, from which the given k-basis is obtainable by the process described above.

Thus the total number of such k-bases of G is equal to $v(G)\, 2^{\binom{k}{2}}$; for with a given composition series ξ_i may be chosen in 2^{i-1} ways.

Now let $\bar{G}$ be the direct product of the k cyclic groups $\{\bar{\xi}_i\}$, where $\bar{\xi}_i$ is of order 2^i. The correspondence $\bar{\xi}_i \to \xi_i$ is a homomorphism of $\bar{G}$ onto G, in which the subgroup $\bar{N}$ of $\bar{G}$ which is generated by the elements

$$(\bar{\xi}_i)^{-2}\, \varphi_i\, (\bar{\xi}_{i+1}, \ldots, \bar{\xi}_k) \qquad (i = 1, 2, \ldots, k-1)$$

corresponds to the identity of G, so that $G \cong \bar{G}/\bar{N}$. And it is easy to see that, if for G we take in turn all $\omega(k)$ groups of $\mathfrak{S}_k$, the total number of subgroups $\bar{N}$ which arise in this way is equal to $2^{\binom{k}{2}}$.

But we can calculate this number in another way, viz. by evaluating the number of distinct subgroups $\bar{N}$ which arise from a particular group G of $\mathfrak{S}_k$, and then summing for all G. In fact, the k-bases of G occur in classes of $t(G)$ each, if we agree to place two k-bases in the same class whenever they can be obtained one from the other by applying a suitable automorphism of G. And two k-bases of G will give rise to the same subgroup $\bar{N}$ if and only if they belong to the same class. Thus, since G possesses as we have seen exactly $v(G)\, 2^{\binom{k}{2}}$ distinct k-bases of the kind in question, it will give rise to just

$$\frac{v(G)}{t(G)}\, 2^{\binom{k}{2}}$$

distinct subgroups $\bar{N}$. Summing for all G of $\mathfrak{S}_k$ and dividing by $2^{\binom{k}{2}}$, we obtain the result required, viz. formula (2).

The proof just given is typical. All our primary formulae, both those already mentioned and those to come, are obtained by a similar line of argument, in that they all depend on the construction of a group $\bar{G}$, of which the groups G of the system $\mathfrak{S}$ are homomorphic images: $G \cong \bar{G}/\bar{N}$. The number of subgroups $\bar{N}$ involved is then calculated in two different ways. First, directly from the structure of $\bar{G}$, which depends only on the system $\mathfrak{S}$ and the arithmetical function n under consideration. Secondly, by finding the number of subgroups $\bar{N}$ corresponding to a given G and summing over all G of $\mathfrak{S}$. It is this second step which produces the factors $t(G)$ in the denominators.

5. The formulae mentioned hitherto have been chosen for the sake of their simplicity. They are, however, only instances of a very wide and general class of arithmetical relations of a similar character. These relations, moreover, are not confined to Abelian groups, which we have been considering so far. But more important is the fact that all our primary formulae can be reduced to a certain *standard form*, which can be written as follows:

$$\sum_R \frac{1}{t(R)} = \frac{1}{t(S)}. \tag{12}$$

In (12), the numbers $t(R)$ and $t(S)$ are integers; they are in fact the orders of certain groups $T(R)$ and $T(S)$, which are in a broad sense groups of automorphisms. But they are not groups of automorphisms of groups. The symbol S stands, not for a group, but for what I shall call a *pure group situation*. On the other hand, R stands for a *realization* (as I shall express it) of the situation S. A given situation has in general several distinct realizations. And the equation (12) is to be interpreted by the statement that *the sum of the reciprocal orders of the groups of automorphisms of the various distinct realizations of a given pure situation is equal to the reciprocal order of the group of automorphisms of the situation itself.*

The remainder of the paper will be devoted to the elucidation of these ideas. And it may be well to beginn by restating one of our previous results, viz. (10), in the above standard form.

The situation $S_1 = S_1(Q_1, Q_2, \ldots, Q_r)$ which gives rise to this formula may be defined as the "Inbegriff" or abstract idea of an Abelian group possessing a chain of subgroups with the prescribed factor groups $Q_1, Q_2, \ldots, Q_r$. Any particular Abelian group G, together with a particular chain of subgroups in it having the prescribed factor groups, constitutes a realization R of S_1. The group of automorphisms $T(R)$ is the group of all automorphisms of G which leave invariant each member of the given chain. And we consider two such realizations, R and R', to be the same if and only if there exists an isomorphism between the groups G and G' which maps the chain defining R onto the chain defining R'.

For a given group G of $\mathfrak{S}^m$, the total number of chains of the specified kind, viz. $v_{Q_1, Q_2, \ldots, Q_r}(G)$, may be split up into classes, two chains belonging to the same class if and only if they are obtainable one from the other by applying a suitable automorphism of G. This means that there is a 1-1 correspondence between the chain-classes of the various groups of $\mathfrak{S}^m$ and the realizations of the situation we are considering.

By an elementary principle of group-theory, if Γ is a class of chains from the group G containing $\tau(\Gamma)$ members, then $\tau(\Gamma)\, t(R) = t(G)$, where R is the corresponding realization. Thus, for the realizations of S_1 which arise from a given group G of $\mathfrak{S}^m$, we have

$$\sum_{R \text{ in } G} \frac{1}{t(R)} = \sum_{\Gamma \text{ in } G} \frac{\tau(\Gamma)}{t(G)} = \frac{v_{Q_1, Q_2, \ldots, Q_r}(G)}{t(G)}. \tag{13}$$

Hence, summing over all G, we see that for the present situation the left-hand side of (12) is equal to $f(v_{Q_1, Q_2, \ldots, Q_r}; \mathfrak{S}^m)$.

It only remains to define $T(S_1)$ to be the direct product of the groups of automorphisms $T(Q_1), \ldots, T(Q_r)$ of the prescribed factor groups, in order to obtain (10) in the required standard form.

6. The situation S_1 just considered is a very special one, particularly with regard to the fact that its "Bestimmungsstücke", viz. the r factor groups Q_i, are mutually independent. It is this fact which justifies our taking the direct product of the $T(Q_i)$ as the group of automorphisms of the situation.

Accordingly, we shall consider next a slightly more intricate example, still from the domain of Abelian groups, in which this particularity is no longer present.

Let A, B and C be any three Abelian groups, of finite orders a, b and c. Let H be an Abelian group of order ab, containing a subgroup B' such that $H/B' \simeq A$ and $B' \simeq B$. Let K be an Abelian group of order bc, containing a subgroup C' such that $K/C' \simeq B$ and $C' \simeq C$. Finally, let θ be a definite isomorphism mapping B' onto the isomorphic group K/C'.

The situation $S_2 = S_2(H, K, B', C', \theta)$ which we wish to consider may now be defined by specifying its realizations. These realizations are Abelian groups G, of order abc, with subgroups P and Q satisfying the following conditions: (i) $G \geqq P \geqq Q \geqq 1$; (ii) $G/Q \simeq H$ and $P \simeq K$; (iii) it shall be possible to choose an isomorphism φ of G/Q with H which maps P/Q onto B', and an isomorphism ψ of P with K which maps Q onto C', in such a way that $\varphi\theta\psi^{-1}$ gives the identical automorphism of P/Q. The realization is thus specified by the chain (i), and its group of automorphisms consists of all automorphisms of G which leave both P and Q invariant.

Two such realizations G, P, Q and G', P', Q' are to be considered the same if and only if there exists an isomorphism mapping G on G', P on P' and Q on Q'.

We have still to define the group of automorphisms of this situation. We may obtain it most simply as a subgroup of the direct product $T(H) \times T(K)$, that is, as a group of pairs $(\eta, \varkappa)$, where η is an automorphism of H and $\varkappa$ an automorphism of K. In order that the pair $(\eta, \varkappa)$ may belong to $T(S_2)$, three conditions must be fulfilled: (i) η must leave B' invariant; (ii) $\varkappa$ must leave C' invariant; and (iii) the automorphisms of B' determined by η and by $\theta\varkappa\theta^{-1}$ must coincide. With this definition of $T(S_2)$, it is easy to verify the formula (12) for the present case.

The situation S_2 is, in fact, determined by the abstract groups H and K, together with the specific relation between them which is described by the data B', C' and θ. And the pairs $(\eta, \varkappa)$ which constitute the group $T(S_2)$ are precisely those which preserve this specific relation, which is an essential part of the definition of the situation.

7. It is evident that, for any realization of $S_2(H, K, B', C', \theta)$, we must have $G/P \simeq A$, $P/Q \simeq B$, $Q \simeq C$. Every such realization will therefore be at the same time a realization of $S_1(A, B, C)$. Conversely, every realization of the latter determines a unique situation of the same general type as S_2, though possibly with different values for H, K, B', C' and θ, which must however satisfy the conditions

$$H/B' \simeq A, \quad B' \simeq K/C' \simeq B \text{ and } C' \simeq C.$$

And it is therefore clear that we must have

$$\sum \frac{1}{t(S_2)} = \frac{1}{t(S_1(A, B, C))} = \frac{1}{t(A)\, t(B)\, t(C)}, \tag{14}$$

the summation being taken over all distinct situations S_2 which satisfy the above conditions.

It should be remarked in connection with (14) that two situations are to be considered the same if and only if they have precisely the same realizations. Thus a situation may be defined by specifying its realizations. And $S_1(A, B, C)$, regarded in this way as the set of its own realizations, is therefore the *sum* (in the set-theoretic sense) of the various distinct situations S_2 which contribute to the left-hand side of (14); and the standard formula for the former may be derived by a corresponding summation from the standard formulae for the latter. We may say that the S_2 here involved are *refinements* of $S_1(A, B, C)$.

Our definition of the identity of two situations leads in the present case to the following result: $S_2(H, K, B', C', \theta) = S_2(H_1, K_1, B_1', C_1', \theta_1)$ if and only if it is possible to choose an isomorphism λ mapping H on H_1 and B' on B_1', and an isomorphism μ mapping K on K_1 and C' on C_1', in such a way that the isomorphism $\lambda\theta_1\mu^{-1}$ of B' onto K/C' coincides with θ.

If for purposes of reference we choose two definite isomorphisms of the groups B' and K/C', respectively, with the abstract group B, then any particular choice of θ determines an automorphism β of B. Moreover, H and B' determine a definite realization R_1 of $S_1(A, B)$, and at the same time a definite subgroup T_1 of the group of automorphisms of B, viz. that which corresponds by our chosen isomorphism of reference to the group of automorphisms of B' defined by $T(R_1)$. Similarly, K and C' determine a definite realization R_1' of $S_1(B, C)$, and a definite subgroup T_1' of $T(B)$. And we have the simple rule that, for given R_1 and R_1', two different choices of θ will give the same situation S_2, if and only if the two corresponding automorphisms β of B belong to the same double coset modd (T_1, T_1') in $T(B)$.

Thus, for given R_1 and R_1', there is a 1-1 correspondence between these double cosets and the various possible situations. Moreover, as is easy to see, the numbers $t(S_2)$ are inversely proportional to the numbers of elements in the corresponding cosets. In fact, if the latter number is m, we have $mt(S_2) = t(R_1)\, t(R_2)$. This gives a simple proof of (14), since, for given R_1 and R_2, $\Sigma m = t(B)$; while

$$\sum \frac{1}{t(R_1)} = \frac{1}{t(A)\, t(B)} \quad \text{and} \quad \sum \frac{1}{t(R_2)} = \frac{1}{t(B)\, t(C)}.$$

The analogy between (14) and (12) is obvious. We may regard the realizations of a given situation S as themselves situations of a special kind; they are *completely determinate situations*, each having only a single realization, and may therefore be described as the ultimate refinements of S, which is their sum. The refinements S_2 which occur in (14), on the other hand, are only partial, and may be themselves refined; for example, by replacing them by their realizations, which would give us the standard formula for $S_1(A, B, C)$.

8. We have discussed the situations S_2 in detail chiefly because they may be used to illustrate a distinction of fundamental importance, bearing on the precise nature of the concept of a group situation. This is the distinction between *pure* and *mixed* situations.

It may well be asked whether in this discussion it would not have been simpler to dispense with the requirements relating to the isomorphism θ, and to consider instead the situation $S_3 = S_3(H, K, A, B, C)$ whose realizations are the chains of subgroups, $G \geqq P \geqq Q \geqq 1$, which satisfy

$$G/Q \simeq H, \quad P \simeq K, \quad G/P \simeq A, \quad P/Q \simeq B, \quad Q \simeq C. \tag{15}$$

Clearly, such a situation as this may be regarded as the sum of a certain number of situations of our former type S_2. And in this way we find, for the realizations R of S_3, the result

$$\sum \frac{1}{t(R)} = \frac{v_{A,B}(H)\, v_{B,C}(K)\, t(B)}{t(H)\, t(K)}. \tag{16}$$

In general, the expression on the right of (16) is not the reciprocal of an integer. And it is therefore impossible to define a group $T(S_3)$ for which (12) holds. In these circumstances, we say that S_3 is a *mixed situation*, in contrast to the *pure situations* S_1 and S_2 for which (12) is valid.

The reason for this distinction is obvious: the various realizations of a mixed situation, such as S_3, do not genuinely "belong together" in an organic sense, as do those of the pure situations which we have considered so far. It is this element of heterogeneity which makes it impossible to define the group of automorphisms of a mixed situation.

We are therefore led to formulate, as a programme for further investigations, the following problems:

(I) To express a given situation S (whether mixed or pure) as a sum of pure situations.

(II) To construct pure situations and to determine their groups of automorphisms.

As to (I), since every S may be regarded as the sum of its realizations, which are themselves pure situations, we always have at least one solution of this problem. If S is mixed, the main interest would naturally lie in finding an expression in terms of as few pure situations as possible. But the analysis of a pure situation into a sum of pure refinements, of which we have given an example in equation (14), may also, I think, lead to results of value.

For instance, if S is mixed, a solution of (I) may enable us to calculate the quantity

$$\left\{\sum \frac{1}{t(R)}\right\}^{-1}, \tag{17}$$

(the sum being taken over all distinct realizations of S) independently of the individual realizations, viz. as

$$\left\{\sum \frac{1}{t(S')}\right\}^{-1}, \tag{17'}$$

where S' runs through the various distinct pure situations whose sum is S. And we shall then obtain a formula of type (1). An example of this is given by (16), the corresponding function $n(G)$ being here the total number of chains $G \geqq P \geqq Q \geqq 1$ in G which satisfy (15); so that the right-hand side of (16) is precisely $f(n; \mathfrak{S}^{abc})$, with this value of n.

For the sake of the formal analogy, we might perhaps agree to call the quantity (17) the *capacity* of the situation S; so that, for a pure situation, the capacity is equal to the order of the group of automorphisms. Then, merely as a matter of definition, in any analysis of S into a sum of pure situations S', the sum of the reciprocal capacities of the situations S' is equal to the reciprocal capacity of S.

An example of this method of obtaining secondary formulae, corresponding to mixed situations, from primary formulae has already been given in the derivation of (8) from (10). Another example is provided by (3), the underlying situation here being that of an ordered pair of composition series of an Abelian group of order 2^k. This is a mixed situation, of capacity $1/k!$, which may be expressed as the sum of $k!$ different pure situations, each of capacity 1, these corresponding to the $k!$ different possible relations of the two composition series in regard to the subgroup lattice which they determine.

9. Hitherto, we have been content to define a situation by specifying its realizations, and to illustrate our ideas by a few simple examples. The general notion of a group situation only acquires a precise meaning, however, once we have stated exactly what is to be understood by a realization, in a form independent of the situation concept itself.

The most natural and convenient definition seems to be the following. A realization is a group G, together with a definite ordered system $G_1, G_2, \ldots$ of subgroups of G. A second realization, given by $G', G_1', G_2', \ldots$, is to be considered identical with the first, if and only if there exists an isomorphism mapping G onto G', and at the same time mapping each of the subgroups G_i onto the corresponding subgroup G_i'.

In the examples considered above, the subgroup systems involved have always had the form of a simple chain extending from G to the identity. But this seems to be an unnecessary restriction of the usefulness of the idea.

We may now define a situation as an arbitrary set of realizations.

It is clear, however, that with this degree of generality, the term has a merely descriptive value. The really interesting question remains that of discovering pure situations, *i. e.* our problem (II). While numerous particular solutions of this problem have come to light, it has unfortunately not proved possible so far to include all known cases under a single general rule. There are, nevertheless, certain features which are common to all the pure situations at present determined; and it may perhaps be of interest to indicate briefly what these are, as a first step towards a definitive solution of the problem.

It seems plausible to assume in the first place that, for any two relizations of a pure situation S, the two subgroup systems shall be in 1-1 correspondence in such a way that corresponding subgroups are of the same order. And in particular, we may suppose that the containing groups G are of the same order for all realizations of S. Further, any system of subgroups of a group G determines a subgroup lattice; and there will clearly be no loss of generality if we take all realizations to be determined by lattices. It is then natural to make the further assumption that, for the realizations of a pure situation, the 1-1 correspondence mentioned above shall be a lattice-isomorphism, preserving the relations of inclusion between subgroups.

These assumptions are all fulfilled in every known case. Furthermore, the latter have the additional property that, in the above lattice, which is the common framework of all the possible realizations, certain specified factor groups are prescribed to within an isomorphism. So that, between any two realizations of a pure situation, we may establish a system of *local isomorphisms*, one for each of the prescribed factors. Moreover, where two of these prescribed factors "overlap", it seems necessary to insist that the two corresponding local isomorphisms shall be consistent, in the sense of giving the same isomorphism of their common portion. This consistency condition has already been illustrated in the discussion of the situations S_2, the prescribed factors being H and K, with B as overlap. Complications arise when several prescribed factors overlap mutually; but these are difficulties of detail. More important is the condition that the prescribed factors shall between them "cover" the whole lattice, a condition which, when properly formulated, ensures the equality of the orders of corresponding subgroups in any two realizations which was mentioned above.

While we cannot, of course, assert that these conditions are necessary for purity of situation, they certainly hold in all cases so far elucidated. And it may be conjectured that, for Abelian situations, they will prove, when stated with the necessary precision, to be sufficient; though difficulties due to the complication of a general modular lattice still stand in the way of formal proof.

In any case, for a pure situation S defined in the way just outlined, the group $T(S)$ may be obtained very simply as follows. As we have explained, for any ordered pair of realizations of S there exists at least one (and in general more than one) system of consistent local isomorphisms between the pairs of corresponding prescribed factors. These systems form a groupoid in the sense of H. Brandt. And $T(S)$ is the corresponding group, which may therefore be defined as the set of all systems of consistent local automorphisms of any given realization of S. Thus $T(S)$ is obtained as a certain subgroup of the direct product of the groups of automorphisms of the prescribed factors.

10. We have chosen our examples so far exclusively from the domain of Abelian groups. We shall conclude with a few remarks on the more complex topic of non-Abelian situations.

The conditions sketched out in the preceding paragraph are certainly insufficient to ensure purity of situation, in general, once we drop the requirement that all the groups involved shall be Abelian. These conditions then need to be supplemented.

For instance, one of the simplest situations in which these conditions hold is that of the extensions of a given group B by a given group A. In this case, A and B are the prescribed factors, and there is no overlapping. But, except in the most trivial cases, this situation is mixed. And it remains mixed, in general, even if we restrict ourselves to a single extension-class, such as is determined by a definite homomorphic mapping of A onto some subgroup of $T(B)$.

A more detailed analysis than it is possible to give here suggests that, in order to obtain the non-Abelian analogues of our pure Abelian situations, we need, as a supplementary condition, to insist that all realizations shall be *isoclinic*, in the sense defined in a previous paper[2]). Indeed, we really need rather more than this; between any two realizations there must exist a definite isoclinism which shall be consistent, in a sense easy to specify, with the system of consistent local isomorphisms whose existence was already postulated for the Abelian case. Thus, in view of the definition of isoclinism given in (C), this new condition amounts effectively to prescribing two new factors, viz. the commutator subgroup and the central quotient group. Though it is true to add that the mutual consistency condition for these two new factors, which is implied in the notion of isoclinism, is of an essentially different character from that which is to relate them to the other prescribed factors, and these among themselves.

Since all Abelian groups are isoclinic, it is perhaps natural to look in this way for pure non-Abelian situations, in the first instance, within the limits of a single family of isoclinic groups. In any case, the supplementary condition given above does in fact enable us to obtain for each family a system of pure situations which are strictly analogous to those of the Abelian family.

The simplest Abelian situation is that whose only realization is the group 1. This group constitutes the *stem* of the Abelian family. We may recall that, for any family Φ, the stem consists of all groups of Φ which are of minimal order; and that the stem-groups are characterised by the property that their centrals Z_1 are contained in their commutator subgroups H_2. Now *the stem of a family is always a pure situation, the realizations of which are the individual stem-groups.*

We may define an *autoclinism* of any group G as an isoclinism of G with itself. It is then easy to show that the various autoclinisms of G form a group, which depends (to within an isomorphism) only on the family Φ to which G belongs. Thus we may call this group the *group of autoclinisms* of the family Φ, and denote it by $U(\Phi)$, and its order by $u(\Phi)$. This group of autoclinisms is precisely the group of automorphisms of the stem-situation S_Φ, so that we may write $U(\Phi) = T(S_\Phi)$. And we therefore have the important formula

$$\sum \frac{1}{t(G)} = \frac{1}{u(\Phi)}, \tag{18}$$

which is simply (12) with $S = S_\Phi$, and where the sum is to be taken over all stem-groups of the family Φ.

---

[2]) *P. Hall*, The classification of prime-power groups, this journal **182** (1940), p. 133. This paper will be referred to as (C).

As a numerical example, consider the family which may be characterised by the fact that the central quotients and commutator subgroups of its members are elementary groups of order 8. The group of autoclinisms of this family is the simple group of order 168. And there are 10 stem-groups (of order 64), the values of $t(G)$ being $2^9\mu$, where $\mu = 21, 6, 6, 6, 6, 3, 2, 2, 2$ and 2.

It is obvious that, if, in determining these stem-groups, one or two groups had been overlooked, or, as might well happen, some had inadvertently been counted twice, then the sum in (18) would be very unlikely, when calculated from such an erroneous set of stem-groups, to come to the correct value of 1/168. Such a result could only be due to an improbable balancing of errors. We have, therefore, in this formula a most delicate test of the correctness of such a determination.

11. The order of a group G of a given family Φ depends solely on the order of its *branch factor-group*

$$Z_1/(Z_1 \wedge H_2) \simeq Z_1H_2/H_2\,, \tag{19}$$

and is equal to this number multiplied by the common order of the stem-groups of Φ. The groups G of Φ for which the order of (19) is m are said to form a *branch* $\mathfrak{S}_\Phi^m$ of Φ.

If Q is a given Abelian group of order m, then the members of $\mathfrak{S}_\Phi^m$ for which (19) is isomorphic with Q, are the realizations of a pure situation S_Φ^Q, whose group of automorphisms is the direct product $T(Q) \times U(\Phi)$. This is the general analogue of the Abelian situation having the group Q as its only realization.

If we sum the standard formulae for the various situations S_Φ^Q, keeping Φ fixed and allowing Q to run through all Abelian groups of order m, we obtain the result

$$f(1;\, \mathfrak{S}_\Phi^m) = \frac{\sigma^{(m)}}{u(\Phi)}; \tag{20}$$

$\sigma^{(m)}$ being the reciprocal capacity of the Abelian groups of order m, regarded as realizations of a mixed situation. (This number may be written down at once with the help of equation (7) and the corresponding results for odd primes.)

When $m = 1$, (20) reduces to (18). It may be used in the same way as the latter to test the correctness of group determinations.

Corresponding to the situations S_1 and S_2 for Abelian groups, we obtain a similar series of pure situations for every family Φ simply by imposing the Abelian conditions on the branch factor-groups (19). Since there is no overlapping between (19) and the factor-groups G/Z_1 and H_2 which are involved in the notion of isoclinism, it follows that the groups of automorphisms of the situations so obtained are the direct products of the groups of automorphisms of the corresponding Abelian situations with the group $U(\Phi)$.

In the general case, however, there exist many new types of pure situation which reduce, for the Abelian family, either to triviality or to one of the types already considered. A single example must suffice.

We shall say that two isoclinic groups G and G', with isomorphic centrals Z_1 and Z_1', belong to the same *situation of centrals*, if there exists an isoclinism θ of G with G' and an isomorphism φ of Z_1 with Z_1' which coincide in their effect on the common portion of their ranges of action, viz. on $Z_1 \wedge H_2$. (This condition implies that φ maps $Z_1 \wedge H_2$ onto $Z_1' \wedge H_2'$, since θ automatically does so.) The situations of centrals defined in this way are pure situations; and the individual groups G which belong to them each give a single realization. The group of automorphisms of the situation may be defined from any particular realization G as the group of all pairs (θ, φ), where θ is an autoclinism of G, and φ is an automorphism of its central Z_1 which coincides with θ in its effect on $Z_1 \wedge H_2$.

Every group G of a given branch $\mathfrak{S}_\Phi^m$ determines a unique situation of centrals to which it belongs. Dually, we may define situations of commutator quotients, which are also pure, like the situations of centrals. We then have two quite different (dual) ways of expressing the mixed situation S_Φ^m as a sum of pure situations, viz. (i) as sum of situations of centrals, and (ii) as sum of situations of commutator quotients. A third expression of this kind has already been mentioned in the derivation of (20), viz. the expression of S_Φ^m as sum of the pure situations S_Φ^Q, with Q of order m.

The standard formulae for the pure situations which are here involved allow us to calculate explicitly, without reference to the individual groups G, the values of the sums $\Sigma 1/t(G)$, taken over the groups of each pure situation separately. We obtain in this way a network of arithmetical relations which must be satisfied by the numbers $t(G)$ for the groups G of the given branch. For each of our three analyses of S_Φ^m, these relations must add up to give (20). But clearly they will provide, in general, far more detailed and delicate tests of the accuracy of a determination of $\mathfrak{S}_\Phi^m$ than that given by equation (20) itself.

For a fuller account and further details, the reader is referred to a forthcoming paper on prime-power groups written in collaboration with Mr. J. K. Senior.

Eingegangen 29. April 1940.

Die Automorphismengruppen der Cayleyzahlen[1]).

Von *Ernst Witt* in Hamburg.

k bezeichne irgendeinen Körper der Charakteristik 0, K sei der Körper der komplexen Zahlen. — Cartans Strukturuntersuchungen der halbeinfachen Lieschen Ringe über K sind von Landherr und Jacobson auf k übertragen worden, wenigstens für den Fall, daß der Liesche Ring über K einer linearen, orthogonalen oder einer Komplex-Gruppe entspricht. Es gibt nach Cartan noch fünf weitere kontinuierliche einfache Gruppen. Zu diesen gehört die 14-gliedrige Automorphismengruppe $\mathfrak{G}_{14}$ der Cayleyzahlen $\mathfrak{C}$. Der $\mathfrak{G}_{14}$ entsprechende Liesche Ring $\mathfrak{L}_{14}$ läßt sich als Menge aller Differentialoperationen von $\mathfrak{C}$ erklären. Umgekehrt zeigt eine längere Rechnung, daß $\mathfrak{C}$ als einziges alternierendes einfaches hyperkomplexes System diese Differentialoperationen gestattet. Diese wechselseitige Beziehung zwischen $\mathfrak{L}_{14}$ und $\mathfrak{C}$ läßt sich von K auf k übertragen. Das Typenproblem der Systeme $\mathfrak{L}_{14}$ über k ist damit auf das bereits von Zorn erledigte Problem der Systeme $\mathfrak{C}$ zurückgeführt. Zur Durchführung der Beweise ist folgender neuer Satz wesentlich: $\mathfrak{L}/k$ sei ein halbeinfacher Liescher Ring. Jede Darstellung $\mathfrak{D}$ in K von $\mathfrak{L}$, deren höchstes Gewicht sich ganzzahlig aus den Wurzeln der regulären Darstellung kombinieren läßt, ist Erweiterung einer eindeutig bestimmten Darstellung $\mathfrak{d}$ in k.

[1]) Bericht über eine Dissertation von Fräulein E. Bannow, Abh. Math. Seminar Hamburg **13** (1940), 240—256.

Eingegangen 2. September 1939.

The construction of soluble groups.

By *P. Hall* in Cambridge (England).

1. Many different methods have been suggested from time to time for the construction of soluble groups, notably by *Jordan*[1]), by *Lunn* and *Senior*[2]) and by *Fitting*[3]). And these methods do in fact enable us to determine many special classes of soluble groups without much trouble. There are two rather serious difficulties, however, which are liable to be met with when we try to push beyond a certain point. There is first the difficulty of factor systems. Secondly, there is the difficulty of isomorphisms, that is, the problem of deciding whether two constructed groups are really the same or not. Before we can consider a construction theory to be completely satisfactory, we must, I think, be able either to overcome or to evade these two major obstacles. And we should expect also of such a theory that it gives definite rules of procedure capable, when followed far enough, of producing any soluble group whatever.

It will probably be agreed that no existing theory quite meets these requirements. And it is therefore not necessarily superfluous if, in the present paper, I give a sketch of yet another scheme, in which a deliberate attempt has been made to avoid the two difficulties referred to. The essence of this plan consists in a combination of two ideas, that of a *partially complemented extension* and that of a *relative system normalizer*. Many details, however, have had to be passed over for reasons of brevity.

2. I will begin by recalling the essentials of the *extension problem*: given the abstract groups H and N, to construct all abstract groups G containing N as a self-conjugate subgroup and such that $G/N \simeq H$.

Let G be such a group. Then we may establish between the elements ξ of H and the cosets of N in G an isomorphism $\xi \leftrightarrow Nd(\xi)$. Every element of G is then uniquely of the form $nd(\xi)$, with n in N and ξ in H. If we write

$$d(\xi)d(\eta) = c(\xi, \eta)\, d(\xi\eta),$$

and

$$d(\xi)n = n^{\theta(\xi)}\, d(\xi),$$

then G is uniquely determined by the *factor system* $c(\xi, \eta)$ and the *automorphisms* $\theta(\xi)$ of N. For, knowing these, we can find the product of any two elements of G from the formula

$$n_1 d(\xi) \cdot n_2 d(\eta) = n_1 n_2^{\theta(\xi)}\, c(\xi, \eta) \cdot d(\xi\eta). \tag{1}$$

The theory of Schreier tells us the conditions which the $c(\xi, \eta)$ and $\theta(\xi)$ must satisfy in order that the law of multiplication (1) shall in fact define a group.

[1]) Mem. Pont. Accad. Rom. dei Nuovi Lincei **26** (1908), 7—39. J. Math. pures appl. (7) **3** (1917), 264—374.
[2]) Amer. J. Math. **56** (1934), 319—327, 328—338, 511—512; **57** (1935), 254—260; **58** (1936), 290—304.
[3]) Jber. DMV **48** (1938), 77—141.

Unfortunately, the complexity of these conditions in the general case seriously impairs the usefulness of the theory as a practical method of group construction. And it is necessary, in order to obtain simple results, to make some additional assumption as to the manner in which G contains N.

The simplest such assumption is that N is a *complemented subgroup* of G, *i. e.* that there exists in G a subgroup D such that $ND = G$ and $N \wedge D = 1$. In this case, G is called a complemented extension of N, and there is no loss of generality in taking the elements $d(\xi)$ to lie in D. If this is done, then all the $c(\xi, \eta)$ are equal to 1, and the existence conditions for a group G defined by (1) now merely require that the correspondence $\xi \to \theta(\xi)$ shall be a homomorphism of H onto some subgroup of the group $T(N)$ of all automorphisms of N.

3. A construction theory based exclusively on complemented extensions, however, would be of somewhat limited application. And it is useful to consider a rather more general idea, that of a *partially complemented extension*.

I shall say that G is a partially complemented extension of N if it contains a subgroup D such that

$$ND = G, \quad D < G. \tag{2}$$

This implies that the meet $N \wedge D = C$ is a proper part of N. When $C = 1$, we have the former case of a complemented extension in the ordinary sense.

If G contains such a *partial complement* D of N, satisfying (2), then we may clearly suppose all the $d(\xi)$ to lie in D. The $c(\xi, \eta)$ will then all belong to C.

D, which is of lower order than G, is then an extension of C by H with the same factor system as the extension G of N. And we may formulate the existence problem for partially complemented extensions as follows: *given the proper subgroup C of N and the extension $D = \Sigma C\, d(\xi)$ of C by H, what conditions must be satisfied by the automorphisms $\theta(\xi)$ of N in order that* (1) *shall define a group*? In this formulation the factor system does not enter explicitly, for it is determined by the structure of the group D which is supposed to be known. The conditions required are:

(i) each $\theta(\xi)$ must leave C invariant and must transform it according to the automorphism $d(\xi)\, C\, d(\xi)^{-1}$;

(ii) for all ξ and η of H, we must have

$$\theta(\eta)\, \theta(\xi) = \theta(\xi\eta)\, \varphi(\xi, \eta),$$

where $\varphi(\xi, \eta)$ is the inner automorphism $c(\xi, \eta)\, N\, c(\xi, \eta)^{-1}$ of N. These conditions clearly correspond to the double role of C, (i) as subgroup of D, (ii) as subgroup of N. Their necessity is obvious. And the verification of their sufficiency offers no difficulty.

Thus, given N, D and C, the problem of constructing G is essentially one of extending a homomorphism. For let T denote the group of all automorphisms of N which leave C invariant. If we associate with each element of C the corresponding inner automorphism of N, we have a homomorphic mapping γ of C onto some subgroup of T. We require to extend this into a homomorphic mapping δ of D onto some subgroup of T, in such a way that each element d of D maps into an automorphism of N transforming C in the same way as d itself does.

The problem may be stated rather more precisely. Let T_0 be the group of all automorphisms of N which leave every element of C invariant, and T_1 the group of all automorphisms of N which leave C invariant and transform it in the same way as some element of D. Then, if C^* is the centralizer of C in D, the known structures of N and D determine a definite isomorphism α of D/C^* with T_1/T_0. On the other hand, if C_0 is the meet of C with the central of N, γ gives an isomorphism of C/C_0 with the subgroup $\gamma(C)$ of T_1.

And our problem is to find all continuations δ of γ which shall be, in the obvious sense, "compatible" with the isomorphism α.

When D is a cyclic group $\{d\}$, the solution is well known. If $d^m = c$ is the least power of d which lies in N, then we must have $\delta(d)^m = \gamma(c)$. On the other hand, $\delta(d)$ must leave c invariant. These two conditions, which are equivalent to (ii) and (i) above, respectively, are sufficient to ensure the existence of G as a cyclic extension of N, of relative order m, defined by the relations $d^m = c$ and $d^{-1}nd = n^{\delta(d)}$ for all n of N.

Another simple case is that in which D is self-conjugate in G. C must then be self-conjugate in N. In this case, the existence conditions are best expressed in terms of the commutators $[d, n] = d^{-1}n^{-1}dn$, which must be elements of C. Here d is any element of D and n any element of N. When either d or n lies in C, the value of $[d, n]$ is given by the structures of N or D, respectively. The problem is to extend the definition of the function $[d, n]$ to all pairs d of D and n of N, in such a way that (i) the correspondence $n \to n[n, d]$ is, for fixed d and varying n, an automorphism $\delta(d)$ of N, and (ii) the correspondence $d \to \delta(d)$ is a homomorphism of D onto some subgroup of $T(N)$. The asymmetry between D and N in these conditions is only apparent.

It would not be difficult to pursue these details further and to formulate a procedure for finding all possible solutions in any given case. Here it must suffice to remark that, for given N and D, the smaller the meet C (or the larger C^*) the easier the construction is likely to be; for this narrows the range of the restrictive isomorphisms α and γ. Thus we shall minimise the labour of computation if we choose our extensions to be as nearly complemented as possible.

4. We shall now consider the application of the method of partially complemented extensions to the construction of soluble groups.

A given soluble group G can, in general, be expressed as a partially complemented extension in many different ways, corresponding to the various possible choices of the subgroups N and D. We therefore run the risk of constructing the same group many times over, and of having to supplement our construction theory by an isomorphism theory which would enable us to select a single representative from each class of isomorphic groups so constructed. Experience seems to show that such an isomorphism theory is likely to raise more difficulties than the construction problem itself.

To avoid these difficulties, we need a general rule for selecting, from each group G of the class with which we are concerned, a unique self-conjugate subgroup $N(G)$ and a unique subgroup $D(G)$ which must be a partial complement of $N(G)$, the uniqueness being understood as to within an automorphism of G. It is natural to seek a solution for which $N(G)$ is some characteristic subgroup of G, and $D(G)$ a member of some characteristic class of conjugate subgroups of G. And we must choose the group functions $N(G)$ and $D(G)$ in a manner which is independent of the individual pecularities of G.

Not every self-conjugate subgroup N of a given group G is partially complemented, as a general rule. A necessary and sufficient condition for the existence of a partial complement of N in G is that N *shall not be contained in the Frattini subgroup* $\varphi(G)$ *of* G, which is defined as the meet of all maximal subgroups of G.

5. Let us consider the case of *nilpotent groups*, that is, groups whose Sylow subgroups are all self-conjugate. In such a group, every maximal subgroup is self-conjugate and of index a prime, so that $\varphi(G)$ contains the derived group of G. Indeed, as H. Wielandt has shown, this is a characteristic property of nilpotent groups. Now there exist nilpotent groups all of whose proper characteristic subgroups are contained in the derived group. Clearly then, such groups cannot be constructed on the principles which I have so far outlined, for they have no proper partially complemented characteristic subgroups.

This does not mean that the method of partially complemented extensions is inapplicable to the construction of prime-power groups. On the contrary, in its simplest form, that of cyclic extensions of relative order a prime, it is the method which has been most widely adopted for this purpose, N being usually taken to be a maximal subgroup of G. For certain special classes of prime-power groups, it is possible to choose this subgroup N as a characteristic subgroup; for example, if G has a unique Abelian subgroup of index a prime, it is natural to identify this subgroup with N. Even in such cases, however, a supplementary isomorphism problem remains to be solved, since the choice of the cyclic group D is still to a large extent arbitrary. At the same time, the simplicity of cyclic extensions renders this isomorphism problem less formidable than in the general case. And, granted a uniform rule for the selection of N, this method is, I think, probably the simplest that is available in such cases.

There is, however, another general method of constructing prime-power groups, based on the classification theory which has been outlined in a previous paper[4]), and which is equally applicable in all cases. This method does not involve the use of cyclic extensions, but depends on the idea of a pure situation[5]), making use of the fact that all realizations[5]) of a pure situation may be obtained as quotient groups of a certain group G determined by the particular situation considered. This method has in fact been applied by Mr. *T. E. Easterfield* to the determination of all regular groups of order p^6, where p is a prime[6]). A detailed account of the method will be published in a later paper, written in collaboration with Mr. *J. K. Senior*. And in what follows we shall deal exclusively with the problem of constructing soluble groups which are not nilpotent, on the supposition that a construction theory is already available for nilpotent groups.

6. Let G be any soluble group, and let its lower central series be

$$G = H_1 > H_2 > H_3 > \cdots > H_k = H_{k+1} = \cdots .$$

We mey call H_k the limit of this series and denote it by H_ω. This subgroup H_ω may be characterised by the property that G/H_ω is nilpotent and every self-conjugate K of G for which G/K is nilpotent must contain H_ω. Thus H_ω is the (unique) minimal self-conjugate subgroup with nilpotent quotient group.

We now define the *lower nilpotent series* of G:

$$G = L_0 > L_1 > L_2 > \cdots > L_n = 1,$$

by the rule that $L_{i+1} = H_\omega\,(L_i)$.

As *Fitting* has shown[7]), there also exists an *upper nilpotent series*

$$1 = U_0 < U_1 < \cdots < U_n = G,$$

which is of the same length n as the lower nilpotent series. U_1 may be defined as the join of all self-conjugate nilpotent subgroups of G, and is itself nilpotent. Thus U_1 is the (unique) maximal self-conjugate nilpotent subgroup of G. The remaining terms of the upper series are then obtained by the rule that $U_{i+1}/U_i = U_1(G/U_i)$.

Any series of self-conjugate subgroups of G,

$$G = G_0 > G_1 > G_2 > \cdots > G_m = 1,$$

---

[4]) *P. Hall*, The classification of groups of prime-power order, this journal **182** (1940).

[5]) For explanations of these terms, see *P. Hall*, On groups of automorphisms, this journal **182** (1940).

[6]) These groups were first determined by *M. Potron*, Paris Dissertation (1904), using another method; however, the results found by these two authors do not agree at all points.

[7]) Jber. DMV. **48** (1938), 77—141.

will be called a nilpotent series if each of the factor groups G_{i-1}/G_i $(i = 1, 2, \ldots, m)$ is nilpotent. For any such series, it is easy to see that

$$G_i \geq L_i, \quad G_{m-i} \leqq U_i,$$

for all i. Thus $m \geqq n$.

We call n the (nilpotent) *length* of G. A nilpotent group is a group of length 1.

Although $L_1 = H_\infty$ is the limit of the lower central series of G, the limit Z_∞ of the upper central series is only equal to U_1 in the trivial case when G is nilpotent, in which case $G = U_1 = Z_\infty$. For groups of length greater than 1, we always have $Z_\infty < U_1$. Z_∞ is usually called the *hypercentral* of G. It has the property that $[Z_\infty, L_1] = 1$, so that every element of the hypercentral is permutable with every element of L_1.

In general, $[U_1, L_1] > 1$. For, as Fitting has remarked, U_1 necessarily contains its own centralizer U_1^*. Thus $[U_1, L_1] = 1$ implies that L_1 is contained in the central of U_1. The lenght of such a group clearly cannot exceed 2. The tetrahedral group, for which $L_1 = U_1$ is a Vierergruppe, is an example of a group of length 2 with this property.

It may be of interest to remark that the characteristic subgroup U_1 can be defined in an entirely different way from that given above, viz. as a meet and not as a join. In fact, an element ξ of G belongs to U_1 if and only if, for every chief series

$$G = G_0 > G_1 > G_2 > \cdots > G_\varrho = 1$$

of G, we have $[G_{i-1}, \xi] \leqq G_i$ $(i = 1, 2, \ldots, \varrho)$. Thus *we may define* U_1 *as the meet of the centralizers of the chief factors of* G.

7. We shall now consider what are the appropriate choices to make for the subgroups $N(G)$ and $D(G)$ in order to construct the non-nilpotent soluble groups G by the method of partially complemented extensions.

It is easy to show[8]) that the Frattini subgroup $\varphi(G)$ satisfies the relation

$$U_1 > \varphi(G) \geqq \varphi(U_1).$$

Indeed, it follows from the results to be mentioned below that not only U_1 but all the terms L_i and U_i $(0 < i < n)$ of both nilpotent series are partially complemented in G. Thus any of these would make an adequate choice for $N(G)$. We shall give reasons for thinking, however, that the lower series provides the more convenient choice.

Before considering the proper choice of $D(G)$, we must recall certain known properties of soluble groups.

In a soluble group G, every Sylow subgroup is complemented. Thus, if the order of G is $p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_r^{\alpha_r}$, where $p_1, p_2, \ldots, p_r$ are distinct primes, we can find a system of r subgroups $S_1, S_2, \ldots, S_r$ of G such that $(G : S_i) = p_i^{\alpha_i}$ $(i = 1, 2, \ldots, r)$. Any such system of r "Sylow complements" will be called a *Sylow system* of G.

The Sylow systems of a soluble group are all conjugate. Thus, if $S_1', S_2', \ldots, S_r'$ is a second Sylow system of G, there exists in G an element ξ such that $\xi^{-1} S_i \xi = S_i'$ for all i.

Suppose now that N is a soluble group contained as a self-conjugate subgroup in the larger group G, and suppose that $S_1, S_2, \ldots, S_r$ is any Sylow system of N. Let $M_G(N)$ denote the subgroup formed by all elements μ of G for which

$$\mu^{-1} S_i \mu = S_i \qquad (i = 1, 2, \ldots, r).$$

Then the conjugacy theorem for Sylow systems has two important corollaries. First, the subgroups $M_G(N)$ form, for given N and G and varying Sylow system of N, a single class of conjugate subgroups of G. Secondly, we have $G = N M_G(N)$.

[8]) *Oystein Ore*, Contributions to the theory of groups of finite order, Duke Math. Journal **5** (1939), 445.

Thus, provided N is not nilpotent, $M_G(N)$ is a partial complement of N in G. To proceed further, we must consider the meet

$$N \wedge M_G(N) = M_N(N) = M(N),$$

which is clearly independent of the containing group G. We shall call $M(N)$ an *absolute system normalizer* of the soluble group N, while $M_G(N)$ will be called a *relative system normalizer* of N (relative to G).

The (absolute) system normalizers of a soluble group have a number of remarkable properties. For example, they may be defined in a way which makes no reference to Sylow subgroups. Consider, in any soluble group G, the class of subgroups H which can be connected with G by a subgroup chain

$$G = G_0 > G_1 > \cdots > G_s = H$$

in such a way that each member G_i $(i = 1, 2, \ldots, s)$ is a maximal but not self-conjugate subgroup of the preceding member G_{i-1}. Every system normalizer $M(G)$ belongs to the class of subgroups thus defined. On the other hand, every subgroup of this class contains at least one system normalizer of G. Thus we may define the system normalizers as the minimal members of this class of subgroups.

For our present purpose, however, it is more important to consider the relations between system normalizers and self-conjugate subgroups. These relations are very precise. In order to state them, I will introduce the following definitions.

If H and K are self-conjugate subgroups of G such that $H > K$, we may call H/K a factor of G. The subgroup D will be said to *cover* H/K if every coset of K in H contains at least one representative from D, *i. e.* if KD contains H. If, on the other hand, the meet $D \wedge H$ is contained in K, then D will be said to *avoid* the factor H/K.

Further, we shall call H/K a *central factor* of G if it belongs to the central of G/K. Among the chief factors of G, we distinguish those which are not central factors of G as *eccentric* chief factors.

We then have the following simple rule. *Every system normalizer of G covers every central factor of G and avoids every eccentric chief factor of G.* Thus, as an immediate corollary, the total number of distinct Sylow systems of G is equal to the product of the orders of the eccentric chief factors in any given chief series of G. For this number is $(G : M(G))$.

This covering and avoidance theorem if of crucial importance for our construction theory of soluble groups.

In the first place, it allows us to improve on the result $G = N M_G(N)$. In fact, *if H/N is any nilpotent factor of G, then $G = N M_G(H)$.* For H/N can then be completely covered by a chain of factors all of which are central factors of H. Thus, by the covering theorem, $M_G(H)$ must cover H/N. But by the conjugacy theorem, as we have already seen, $M_G(H)$ must cover G/H. Hence $M_G(H)$ covers G/N, which is the result stated.

The importance of this result for our present purpose comes from the fact that $M_G(H)$ will be, in general, a proper subgroup of $M_G(N)$; although it is still, like the latter, a partial complement of N in G.

It is now clear that all our requirements for a construction theory of soluble groups, based on the method of partially complemented extensions, will be fulfilled if we take either

(1) $$N(G) = L_i, \quad D(G) = M_G(L_{i-1})$$

for a suitable value of i, $0 < i < n$; or alternatively

$$N(G) = U_i, \quad D(G) = M_G(U_{i+1}). \tag{2}$$

For L_{i-1}/L_i and U_{i+1}/U_i are both nilpotent factors of G.

Since the lengths of L_i and $M_G(U_{i+1})$ are both equal to $n-i$, while those of U_i and $M_G(L_{i-1})$ are both equal to i, it follows that the lengths of the groups N and D on which the construction of G is to be based are in every case smaller than the length n of G. This gives the method a character of recurrence. Assuming the groups of length less than that of G to have been already determined, N and D may be taken as known.

8. We have still to consider one important point before our present outline can be regarded as in any way complete. Suppose for the sake of definiteness that we are proposing to construct the soluble groups G of length n by taking $N = L_1(G)$ and $D = M(G)$. We must begin by selecting for N a group of length $n-1$ and for D a nilpotent group. But it is clear that not every extension G of N containing D as a partial complement of N will actually provide a solution of our problem. For we have to ensure that, in the constructed group, D will be a system normalizer and N the limit of the lower central series. To obtain this result, certain conditions must be imposed on the details of the construction, conditions which incidentally greatly reduce the number of cases requiring consideration.

These conditions are most easily expressed in terms of the homomorphism δ which, with our previous notation, maps D onto some subgroup $\delta(D)$ of the group of automorphisms of N.

It is clear that the choice of the subgroup $\delta(D)$ will determine once for all those self-conjugate subgroups of N which are to remain self-conjugate in G. These are the subgroups which are both self-conjugate in N and at the same time invariant under $\delta(D)$. Thus $\delta(D)$ will, in particular, determine those subgroups H of N for which N/H is to become a chief factor of G. And in order that N shall be equal to $L_1(G)$, it is necessary and sufficient that each of these chief factors N/H shall be eccentric; for G/N, being isomorphic with a quotient group of D, will in every case be nilpotent. But the eccentricity or otherwise of the factors N/H is also completely determined by the choice of $\delta(D)$. And our first condition may therefore be stated as follows: $\delta(D)$ must be so chosen that N is the limit of the lower central series of the group $N\delta(D)$, which may be regarded as a subgroup of the holomorph of N. This condition will ensure that $N = L_1(G)$; and, to apply it, we merely need a knowledge of the group of automorphisms of N.

We must now consider how to ensure that D becomes a system normalizer of G. The Sylow system $S_1, S_2, \ldots, S_r$ of G which D is to leave invariant will meet N in a Sylow system $S_1', S_2', \ldots, S_r'$ of N, whose absolute normalizer we denote by M_1. Clearly then, we must insist that $\delta(D)$ shall leave invariant a certain Sylow system of N, the particular choice of which is irrelevant owing to the conjugacy theorem. This, coupled with the nilpotency of D, will suffice to ensure that D is at least contained in a certain system normalizer M of G, the corresponding Sylow system being that which is determined by the chosen Sylow system of N and the unique Sylow system of the nilpotent group D.

In order to make sure that D actually coincides with M, we have now only to arrange that it shall cover all central chief factors of G which are contained in some selected chief series of G. For then, by the covering theorem, the orders of D and M will be the same. Now the construction itself ensures that D will cover G/N. We have therefore only to consider the meet $C = D \wedge N$.

Let η be any element of C of order a prime p. Clearly η must belong to M_1; and in addition it must be transformed into itself by every element of $\delta(D)$ which is of order prime to p. But these two conditions together suffice to ensure that η belongs to M. Thus, if we take for C the group generated by all such elements η, taking for p in turn all relevant primes, we shall have $C = M \wedge N$; and therefore this C will have all the required covering properties. Thus, with this choice of C, we shall in fact have $D = M$.

It will be evident from this discussion that probably the simplest procedure is as follows. First select N. Then choose the nilpotent subgroup $\delta(D)$ from the group of automorphisms of N, subject to the conditions (i) that $\delta(D)$ shall leave a certain Sylow system of N invariant, and (ii) that $N = L_1(N\delta(D))$ as explained above. The choice of $\delta(D)$ determines uniquely the subgroup C of N, and also incidentally the homomorphism γ of C onto $\gamma(C) = \delta(C)$. The final step is then the selection of the nilpotent group D as an extension of C, together with the choice of the homomorphism δ of D onto $\delta(D)$ in such a way that it coincides with γ as regards the elements of C. For the sake of brevity, we shall omit a more detailed consideration of this last step.

If, instead of taking $N = L_1$, we prefer to base the construction on some other assumption such as $N = L_i$ or $N = U_i$, the above process can be adapted without difficulty. It is easy to show that in every case $\delta(D)$ must be of the same length as D, namely, i for $D = M_G(L_{i-1})$, or $n - i$ for $D = M_G(U_{i+1})$. It must be chosen as a subgroup of the group of automorphisms of N leaving invariant a certain Sylow system of N. In addition, it must satisfy the conditions $N = L_i(N\delta(D))$ or $N = U_i(N\delta(D))$, according to the case. Finally, if the upper nilpotent series is used, the homomorphism δ must be such that no element of D not in C is mapped on the identity of $\delta(D)$. Here, as before, C is determined as a subgroup of N by the choice of $\delta(D)$.

On the whole, it may be suggested that the use of the lower nilpotent series is likely to be preferable to that of the upper, for with the former there is, in general, less overlapping of N and D. Indeed it is clear that we could replace $N = U_i$ by $N = L_1(U_{i+1})$, while retaining $D = M_G(U_{i+1})$. Since $L_1(U_{i+1})$ is, in general, a proper subgroup of U_i, we should then have a construction method with less overlapping than before. With $N = L_i$, however, no such reduction of overlapping is possible, since $L_i = L_1(L_{i-1})$.

9. We shall conclude by mentioning briefly a special, though quite extensive, class of soluble groups which can be constructed by our method without any of the complications which arise from the overlapping of N and D. In other words, for the groups of this class, the method of fully complemented extensions is adequate; and genuinely partial complements need not be considered.

The soluble groups in question are those whose Sylow subgroups are all Abelian. Such groups we will call *A-groups*. Among A-groups occur all groups of square-free order; or, more generally, all groups whose Sylow subgroups are all cyclical. These form a special and rather trivial class, since, as is well known, their lengths cannot exceed 2. The length of a general A-group can be arbitrarily large, though it cannot exceed the number of different primes which divide its order.

It is evident that in an A-group every nilpotent factor must be Abelian. Hence the lower nilpotent series coincides with the derived series. In particular, L_1 is the commutator subgroup.

In a general soluble group, there is as a rule no unique maximal self-conjugate Abelian subgroup. In an A-group, on the other hand, U_1 is Abelian and contains every other self-conjugate Abelian subgroup.

The most important property of A-groups for our present purpose is that the meet of the central and the derived group is the identity. More generally, *in an A-group*

G, the derived group L_1 contains no central factor of G. Incidentally, the central of an A-group coincides with its hypercentral: $Z_1 = Z_2 = \cdots = Z_\alpha$.

From this and the avoidance theorem it follows that *the absolute system normalizers of an A-group are all complementary to the derived group.* More generally, every subgroup K of an A-group G which is the derived group of some self-conjugate subgroup H of G is complemented in G. To be precise,

$$K \wedge M_G(H) = 1, \quad KM_G(H) = G.$$

In particular, since L_i is the derived group of L_{i-1}, it follows that the system normalizers of L_{i-1} relative to G are all complementary to L_i. Thus, if we base our construction method on the assumptions $N = L_i$ and $D = M_G(L_{i-1})$, we obtain the A-group G as a complemented extension of N by D, so that $D \simeq G/N$. For instance, all soluble groups of cube-free order may be dealt with in this way.

A-groups have a number of other interesting properties. For example, U_1 is the direct product of the centrals of the various groups of the derived series:

$$U_1 = Z_1(G) \times Z_1(L_1) \times Z_1(L_2) \times \cdots .$$

There is also a basis theorem. Every A-group G contains a system of subgroups $G_1, G_2, \ldots, G_\varrho$ with the following properties:

(i) Each G_i is Abelian, of prime-power order $p_i^{\alpha_i\beta_i}$, and with all its invariants the same, $(\alpha_i, \alpha_i, \ldots, \alpha_i)$.

(ii) Every element of G is uniquely expressible in the form $\xi_1 \xi_2 \cdots \xi_\varrho$, with ξ_i in G_i. Thus the order of G is equal to the product of the orders of the G_i's.

(iii) For every pair G_i, G_j, at least one is contained in the normalizer of the other. Thus the G_i are all permutable.

(iv) Any product of a selection of the G_i's gives a subgroup which is complementary in G to the product of the remainder.

(v) Among such products occur all the terms L_i of the derived series of G, also a complete set of relative system normalizers $M_{L_i}(L_j)$, $i < j$, as well as (obviously) a complete set of Sylow subgroups for each such product.

(vi) Each G_i either covers or avoids any given chief factor of G. And there exists a chief series of G with the property that each of its factors is covered by just one of the G_i's and is avoided by all the rest, G_i covering α_i distinct factors which are all of order $p_i^{\beta_i}$.

Eingegangen 5. Mai 1940.

Bericht über die Arbeit von H. Fitting,

Beiträge zur Theorie der Gruppen endlicher Ordnung.

Von *B. L. van der Waerden* in Leipzig.

Die wichtigsten Grundgedanken der Arbeit sind folgende:

1. Jede endliche Gruppe ist zusammengesetzt aus einem maximalen auflösbaren Normalteiler und dessen halbeinfacher Faktorgruppe.

2. Um die Struktur einer halbeinfachen Gruppe zu erkennen, bilde man ihren Sockel, d. h. ihren maximalen vollreduziblen Normalteiler. Dieser ist das direkte Produkt von nichtabelschen einfachen Gruppen, und sein Zentralisator ist Eins. Daher ist die ganze Gruppe isomorph zu einer die inneren Automorphismen umfassenden Untergruppe der Automorphismengruppe des Sockels.

3. Um die Struktur einer auflösbaren Gruppe zu erkennen, bilde man ihren maximalen nilpotenten Normalteiler $\mathfrak{N}$. Dieser ist das direkte Produkt seiner Sylowgruppen, und sein Zentralisator ist sein Zentrum. Daher ist die Faktorgruppe nach $\mathfrak{N}$ isomorph zu einer Untergruppe der äußeren Automorphismengruppe von $\mathfrak{N}$. Aus dieser Faktorgruppe und dem Normalteiler $\mathfrak{N}$ setzt sich dann die auflösbare Gruppe mit Hilfe eines Faktorensystems zusammen.

Eingegangen 18. Juli 1939.

Zur Abelschen Durchkreuzung.

Von *Arnold Scholz* in Kiel.

Die in meiner Abhandlung „Abelsche Durchkreuzung“ (Furtwängler-Festband der Monatsh. f. Math. u. Phys.) definierten Begriffe *Gruppengeschlecht* und *Klasse verwandter Gruppen* stimmen mit den Hallschen Begriffen *family* und *branch* genau überein, falls der Multiplikator $\mathfrak{M}$ meiner Aufspaltung $\mathfrak{L} = \mathfrak{N} \cdot \mathfrak{M}$ von $\mathfrak{N}$ das volle Zentrum von $\mathfrak{L}$ wird. Die bei mir entstehende Begriffserweiterung ist vom Standpunkt der abstrakten Gruppentheorie unwesentlich, besteht nur in gewissen Unterteilungen der *families* und *branches* und wird erst sinnvoll, wenn $\mathfrak{N}$ als konkrete Gruppe, etwa Galoisgruppe, gegeben ist. Die bei mir mittels Abelscher Durchkreuzung definierte *Klasse* kann man bei endlichen Gruppen natürlich auch durch Zusammenfassung der Gruppen gleicher Ordnung eines Geschlechts definieren. Den *minimal branches* entsprechen die nach dem Konstruktionsbeweis meines Satzes 5, in dessen Formulierung zu wenig gesagt ist, existierenden *Knotungen*; es gilt danach der

Satz. *Jedes Geschlecht zentraler Aufspaltungen enthält genau eine Klasse von Knotungen* (*Minimalklasse des Geschlechts*). *Die Ableitungsanteile aller Multiplikatoren des Geschlechts sind also, weil untereinander isomorph, zum Darstellungsmultiplikator homomorph.*

(In (4) muß dabei $\simeq$ statt $=$ stehen.)

Der Beweis des für Satz 5 nötigen Satzes 3 geht einfacher: Es brauchte nur die Existenz eines Abelschen $\mathfrak{A} \cdot \mathfrak{B} \cdot \mathfrak{C}$ bei gegebenem $\mathfrak{A} \cdot \mathfrak{B}$ und $\mathfrak{B} \cdot \mathfrak{C}$ bewiesen zu werden. Sind nun $A_1, \ldots, A_r$; $B_1, \ldots, B_s$; $C_1, \ldots, C_t$ Basen für $\mathfrak{A}, \mathfrak{B}, \mathfrak{C}$ und a_1 bis c_t die Ordnungen der Basiselemente, so bestehen in $\mathfrak{A} \cdot \mathfrak{B}$ Relationen

$$A_i^{a_i} = F_i(B_j);\ B_i^{b_i} = 1 \quad \text{und} \quad B_i^{b_i} = G_i(C_j);\ C_i^{c_i} = 1$$

in $\mathfrak{B} \cdot \mathfrak{C}$. Sodann ist

$$\{A_1, \ldots, A_r;\ B_1, \ldots, B_s;\ C_1, \ldots, C_t\} \text{ mit } A_i^{a_i} = F_i(B_j);\ B_j^{b_j} = G_j(C_k);\ C_k^{c_k} = 1$$

eine Gruppe $\mathfrak{A} \cdot \mathfrak{B} \cdot \mathfrak{C}$; denn da in $\mathfrak{A} \cdot \mathfrak{B}$ nichts konjugiert ist, entstehen in $\mathfrak{C}$ keine Ordnungsbeschränkungen, und jedes Element in $\mathfrak{A} \cdot \mathfrak{B} \cdot \mathfrak{C}$ ist eindeutig darstellbar als Produkt der A_1 bis C_t mit nichtnegativen Exponenten $< a_i, b_j, c_k$.

Der Beweis der Beschränktheit der Knotungen für Satz 4 wurde unter Verwendung der Abelschen Durchkreuzung von Abelschen auf zyklische Multiplikatoren zurückgeführt und für diese wie üblich durch monomiale Darstellungen bewiesen. Einen dem körpertheoretischen Standpunkt angepaßten einfacheren Beweis erhält man mit der Verlagerung:

Ist $\mathfrak{H} = \mathfrak{G} \cdot \mathfrak{C}$ mit $\mathfrak{C} = \{C\}$ und $\mathfrak{G} = \sum_{i=1}^{n} S_i$, so ist die Verlagerung

$$V_{\mathfrak{H} \to \mathfrak{C}}(C) = C^{\Sigma S_i} = C^n,$$

falls C im Zentrum liegt, aber $= 1$ für $C < \mathfrak{H}'$, also $C^n = 1$, wenn beides eintritt. (Verlagerung eindeutig mod $\mathfrak{C}' = 1$!)

Eingegangen 2. September 1939.

Totale Normenreste, die keine Normen sind, als Erzeuger nichtabelscher Körpererweiterungen. II.

Von *Arnold Scholz* in Kiel.

Allgemein soll hier erörtert werden, wie der Knoten eines Normalkörpers K/K_0 mit der absoluten Galoisstruktur der Klassenkörper von K zusammenhängt.

Knoten von K/K_0 (oder *von* K, wenn der Grundkörper K_0 festliegt) heißt nach der Abhandlung I dieses Titels[1]) die Faktorgruppe H_0/N_0 zweier Zahlgruppen aus K_0, der Gruppe H_0 der totalen Normenreste nach der Gruppe N_0 der Normen von Zahlen aus K.

Totaler Normenrest heißt dabei eine Zahl, die nach jedem Modul, auch nach den unendlichen Primstellen, kongruent einer Norm ist.

Die weiteren hier neu auftauchenden gruppen- und körpertheoretischen Begriffe sind in der Abhandlung „Abelsche Durchkreuzung“[2]) definiert, die überhaupt die gruppentheoretische Grundlage für die vorliegende Abhandlung bildet. Auf Abh. I wird hingegen nicht weiter zurückgegriffen.

Aus F. wiederholen wir die Definition der folgenden körpertheoretischen Begriffe:

Knotung heißt eine zentrale Erweiterung, die keine Abelsche Erweiterung enthält, *zentrale* Erweiterung von K ein Körper Z, dessen Relativgruppe über K im Zentrum seiner absoluten Galoisgruppe liegt („absolut“ immer bezogen auf K_0), *Abelsche Erweiterung* aber ein Körper KA, wo A ein absolut Abelscher Körper, für den rationalen K_0 also ein Kreiskörper ist. (Im Fall einer bloß *relativ* Abelschen Erweiterung fügen wir „relativ“ hinzu oder sprechen meist von einem *Klassenkörper*.) Ferner definieren wir:

Zyklische Verlängerung (= indirekte zyklische Aufspaltung) von K heiße das Produkt von K mit einem zyklischen Körper, der mit K einen echten Teilkörper gemein hat. (Verlängerung überhaupt bedeute eine Aufspaltung, bei der die Basis oder das Erzeugendensystem der Gruppe nicht verbreitert wird.)

Für die Klassenkörper von K verwenden wir folgende Namen und Bezeichnungen: Es sei $\overline{K}$ *der absolute* Klassenkörper, d. h. der volle Klk. mod 1, und $\overline{K}(\mathfrak{m})$ der (volle) Klk. mod $\mathfrak{m}$, besonders $\overline{K}(-1) = \widetilde{K}$ der Klk. mod -1, wo -1 die unendliche rationale Primstelle bezeichnet (mit Rücksicht auf einheitliche Bildung quadratischer Körper; es heiße „quadratischer Rest von -1“ eine positive Zahl).

Der *zentrale Klassenkörper*[3]) *von* $K \bmod \pm 1, \mathfrak{m}$ oder innerhalb eines Klassenkörpers Λ/K sei der maximale Teilklassenkörper der Art, der noch eine zentrale Erweiterung von K ist, und werde mit $\overline{K}^*$, $\widetilde{K}^*$, $\overline{K}^*(\mathfrak{m})$ je nach dem Modul oder Λ^* bezeichnet.

[1]) J. f. M. **175** (1936), S. 100—107.

[2]) Monatsh. f. Math. und Phys. **48** (Furtwängler-Festband 1939), im folgenden mit F. zitiert.

[3]) Bezeichnung stimmt überein mit N. Tschebotarëw: Zur Gruppentheorie des Klassenkörpers, J. f. M. **161** (1929), 179—193, dort durch die vorhandene Trägheitsmasse gekennzeichnet, meist nur für *einfache* Körpererweiterung; vgl. auch [15]).

Der *Geschlechterklassenkörper*[3]) $\overline{K}^0$, $\widetilde{K}^0$, $\overline{K}^0(\mathfrak{m})$ mod ± 1, $\mathfrak{m}$ sei der maximale Teilklassenkörper, der noch eine Abelsche Erweiterung von K ist. — Dagegen bezeichne K^0 den maximalen Abelschen Teilkörper von K; es ist dann $\overline{K}^0 = K(\overline{K})^0$ und $K\Lambda^0$ der in einem Klassenkörper Λ von K liegende Geschlechterklk.

Ein zentraler usw. Klk. bedeute wie üblich einen Teilkörper *des* (vollen) Klk.s seiner Art.

Alphabetverwendung: L Galoissubstitution, L Zahlgruppe, Λ Zahlkörper, $\mathfrak{L}$ Galoisgruppe, l Rationalzahl, $\mathfrak{L}$ Idealgruppe, λ Körperzahl, $\mathfrak{l}$ Ideal

(meist korrespondierend, z. B. wenn L Trägheitssubstitution, so eines Primteilers von l).

Uns interessieren hier vor allem zwei Fragen, deren erste durch Satz 3 und 6 beantwortet wird:

1. Welches sind die Gruppen, die gleich den zyklischen die Eigenschaft haben, daß jeder Galoiskörper K/K_0 mit einer solchen Gruppe *knotenfrei* ist, d. h. daß in ihm der für zyklische Körper zutreffende Satz (vgl. den Anfang von Abh. I) gilt, daß jeder totale Normenrest Norm ist? Wie sich herausstellt, sind das die *abgeschlossenen* Gruppen: die, die ihre eigenen *Darstellungsgruppen* sind.

2. Läßt sich, wenn K einen von der Identität verschiedenen Knoten besitzt, so wie in den Sonderfällen der Abhandlung I eine Erweiterung K' von K finden, deren Gruppe eine *Knotung* der Gruppe von K mit einem zum Knoten isomorphen Multiplikator ist (Multiplikator ist die Gruppe von K'/K), und beruht auch umgekehrt eine vorgelegte Galoisknotung K'/K_0 von K/K_0 auf einem entsprechend großen Knoten von K in K_0?

Beides ist zwar häufig, doch nicht immer der Fall, wie die folgenden Sätze und die Beispiele auf S. 229 zeigen. Zuerst gilt

Satz 1. *Es sei* K *ein Normalkörper über* K_0 *mit dem Knoten* H_0/N_0, *und es seien* H *und* N *die Gruppen der Ideale in* K, *deren Normen in den Hauptidealgruppen* (H_0) *und* (N_0) *liegen. Dann ist der zu* H *gehörige Klassenkörper der absolute Geschlechterklassenkörper*[3]) $\overline{K}^0$ *von* K/K_0, *der zu* N *gehörige Klassenkörper aber der zentrale Klassenkörper* $\overline{K}^*$.

H ist dabei das *Hauptgeschlecht* der absoluten Idealklasseneinteilung in K im Sinne von Hasse, Klassenkörperbericht Ia, S. 296, und N besteht aus den Quotienten konjugierter Klassen.

Gewonnen ist hier vorerst eine Knotung $\overline{K}^*$ von $\overline{K}^0$, deren Relativgruppe außerdem nur zum *Idealknoten* $(H_0)/(N_0)$ isomorph ist und nur dann zum *Zahlknoten* H_0/N_0 isomorph, wenn die Einheitengruppe E_0 knotenfrei ist, also der Durchschnitt $[E_0, H_0] = [E_0, N_0]$ ist. Im anderen Falle eines *Einheitenknotens* $[E_0, H_0]/[E_0, N_0]$ ist aber wie in Abh. I Isomorphie mit dem Zahlknoten durch Klassenkörper einer bestimmten Schar von Führern (vgl. den Charakter ψ in [4]), S. 173) zu erreichen; es gilt

Satz 2. *Hat der Körper* Γ/K_0 *einen Knoten* K *und die Galoisgruppe* $\mathfrak{G}$, *so gibt es eine zentrale Erweiterung* Λ *von* Γ *mit einer Gruppe* $\mathfrak{L} = \mathfrak{G} \cup \mathfrak{C}$, *deren Multiplikator* $\mathfrak{C}$ *mit der Ableitung* $\mathfrak{L}'$ *einen zu* K *isomorphen Durchschnitt* $\mathfrak{M}$ *hat, und es erscheint* Λ *als Knotung eines Geschlechterklassenkörpers* ΓA *mit* $\mathfrak{M}$ *als Relativgruppe.*

Der Führer $\mathfrak{f}$ von Λ/Γ kann dabei zu einem vorgegebenen Ideal $\mathfrak{v}$ teilerfremd gewählt werden.

Mit Hilfe von F., Satz 5 (vgl. auch den Satz der dieser Abhandlung vorangehenden Note) folgt hieraus

Satz 3. *Der Knoten eines Normalkörpers* K *mit der Gruppe* $\mathfrak{G}$ *ist homomorph zum Multiplikator ihrer Darstellungsgruppe* (*isomorph zum Multiplikator einer Knotung von* $\mathfrak{G}$).

[4]) A. Scholz, Konstruktion von Körpern mit beliebiger auflösbarer Gruppe, Math. Zeitschrift **42** (1937), 161—188.

Die Ordnung des Knotens ist somit durch die Struktur von $\mathfrak{G}$ *beschränkt, und* K *ist knotenfrei, wenn* $\mathfrak{G}$ *abgeschlossen ist.*

Die eingangs gestellte Frage 1 ist hiermit zur Hälfte beantwortet. Für die Frage 2 liefert aber Satz 2 nur erst eine Knotung einer Abelschen Erweiterung von K, nicht aber schon eine entsprechende Knotung von K selbst. Gruppentheoretisch läßt sich nun zwar, wie beim Beweis von F., Satz 5, die Abelsche Erweiterung herausheben: es gibt im *Geschlecht* der Gruppe $\mathfrak{L}$ oben in Satz 2 eine Klasse von Knotungen von $\mathfrak{G}$ mit zu $\mathfrak{M}$ isomorphem Multiplikator, die Faktorgruppen einer Abelschen Aufspaltung von $\mathfrak{L}$ sind; doch ist es möglich, daß gerade diese Aufspaltung von $\mathfrak{L}$, bewirkt durch eine Aufspaltung des Abelfaktors $\mathfrak{G}^0$, körpertheoretisch nicht realisierbar ist, nämlich auf eine unlösbare Abelsche Einbettungsaufgabe für den Abelschen Teilkörper K^0 von K führt, wie die Beispiele unter $a = 0$ auf S. 229 zeigen. Wir wollen nun, indem wir in der Frage der Abelschen Einbettung auf [5]) verweisen, vorzüglich den Fall betrachten, daß die nötigen Abelschen Erweiterungen vorgenommen werden können, und definieren:

Geschmeidig heiße ein Normalkörper K mit der Gruppe $\mathfrak{G}$, wenn sein voller Geschlechterklassenkörper Abelsche Erweiterungen von jedem Galoistyp zuläßt, dessen Multiplikator (Relativgruppe über $\overline{\mathsf{K}}^0$) zum Multiplikator $\mathfrak{M}$ der Darstellungsgruppen von $\mathfrak{G}$ homomorph ist. Hierzu genügt die Erweiterbarkeit jedes zyklischen Teilkörpers von $\overline{\mathsf{K}}^0$ zu einem zyklischen Körper vom Relativgrad m, wenn m die Maximalordnung in $\mathfrak{M}$ ist.

Geschmeidig genug heiße K hingegen, wenn die obige Bedingung für seinen Knoten statt für $\mathfrak{M}$ erfüllt ist, und geschmeidig genug für eine bestimmte Knotung unter denselben Bedingungen für deren Multiplikator statt $\mathfrak{M}$. Sodann gilt

Satz 4. *Ist der Körper* K *geschmeidig genug, so gibt es eine Knotung* N *von* K, *deren Relativgruppe zum Knoten von* K *isomorph ist. Die Galoisgruppen der Abelschen Durchkreuzungen von* N *durchlaufen dabei eine volle Klasse verwandter Knotungen.*

Ist auch hier, wie gerade bei den Beispielen auf S. 229, Verzweigungsfremdheit von N/K zu K/K_0 nicht immer zu erreichen, weil man zur Abspaltung des Geschlechterklassenkörpers zyklische Verlängerungen braucht, so zeigt doch die Erreichbarkeit der Verzweigungsfremdheit bei einer Satz-2-Existenz schon, daß sich nicht immer alle zentralen Erweiterungen eines Körpers K auf seinen Knoten beziehen lassen; denn oft vergrößert eine Trägheitssubstitution von $\mathfrak{G}$ bei jeder zentralen Aufspaltung ihre Ordnung, und das zugehörige Primideal muß sich weiterverzweigen. Da nun aber jede zentrale Erweiterung von K ein Klassenkörper über K ist, zu dessen Idealgruppe alle Ideale $\equiv 1$ nach seinem Führer $\mathfrak{f}$ gehören, so reicht zur Erfassung aller zentralen Erweiterungen von K folgende Verallgemeinerung des Knotenbegriffs aus:

$\mathfrak{t}$-*Strahlknoten* oder $\mathfrak{t}$-Knoten von K/K_0 heiße die Faktorgruppe $H_0(\mathfrak{t})/N_0(\mathfrak{t})$ der totalen $\mathfrak{t}$-Strahlnormenreste nach den $\mathfrak{t}$-Strahlnormen und dabei

$\mathfrak{t}$-*Strahlnorm* eine Zahl α_0 aus K_0, die in K Norm einer Zahl $\alpha \equiv 1 \bmod \mathfrak{t}$ ist,

$\mathfrak{t}$-*Strahlnormenrest* mod $\mathfrak{m}$ eine Zahl, die mod $\mathfrak{m}$ einer $\mathfrak{t}$-Strahlnorm kongruent, und *totaler* $\mathfrak{t}$-*Strahlnormenrest* ein γ_0, das nach jedem $\mathfrak{m}$ einer Strahlnorm kongruent ist.

Wert hat die Definition nur für *invariantes* $\mathfrak{t}$ und bei den Normenresten für Vielfache $\mathfrak{m}$ von $\mathfrak{t}$, während sie bei $(\mathfrak{m}, \mathfrak{t}) = 1$ nicht mehr als Normenrest mod $\mathfrak{m}$ bedeutet. Es gilt nun

Satz 5 (vgl. auch die Gruppierung A., B., C. der einzelnen Aussagen im Beweis S. 224). *Für in* K/K_0 *unverzweigtes* $\mathfrak{t}$ *ist der* $\mathfrak{t}$-*Strahlknoten dem Knoten von* K/K_0 *isomorph*

[5]) H. Richter, Über die Lösbarkeit des Einbettungsproblems für Abelsche Zahlkörper, Math. Ann. **112** (1936), S. 700—726.

und stets der (-1)*-Strahlknoten (Vorzeichenknoten). Es gibt in* K *ein Ideal* $\mathfrak{v}$ *der Eigenschaft, daß zum* $\mathfrak{v}$*-Strahlknoten alle* $\mathfrak{w}$*-Strahlknoten isomorph für* $\mathfrak{v}|\mathfrak{w}$ *und sonst wenigstens homomorph sind, und zwar ein* $\mathfrak{v}$*, dessen Primteiler in* K *verzweigt sind.*

Jede zentrale Erweiterung Λ von K *hat über der in ihr enthaltenen Abelschen Erweiterung* $\mathsf{K}\Lambda^0$*, falls verzweigungsfremd, eine zum* 1*-Knoten und allgemein eine zum* $\mathfrak{v}$*-Strahlknoten homomorphe Gruppe. Für gewisse* Λ *gilt Isomorphie. Bei geschmeidigem* K *haben schon die maximalen Knotungen von* K *eine zum Strahlknoten isomorphe Relativgruppe.*

Schließlich gilt

Satz 6. *Zu jeder Gruppe* $\mathfrak{G}$ *gibt es Körper* K_0 *und* K*, für die* K *über* K_0 *eine Gruppe der Struktur* $\mathfrak{G}$ *hat und einen zum Darstellungsmultiplikator von* $\mathfrak{G}$ *isomorphen Knoten.*

Wir bringen jetzt die Beweise der Sätze 1—6, beweisen aber vorerst das

Kriterium (Satz 7[1]). *Ein Klassenkörper* Λ *von* K *mit der Idealgruppe* I *ist, bezogen auf einen Körper* K_0*, über dem* K *Normalkörper ist,*

ein Geschlechterklassenkörper (eine Abelsche Erweiterung) genau dann, wenn in K *die Zugehörigkeit eines Ideals* $\mathfrak{i}$ *zur Idealgruppe* I *nur von der Kongruenzklasse seiner Norm* $\mathfrak{i}_0 \bmod \mathfrak{m}_0$ *abhängt und dabei* $\mathfrak{m}_0$ *in* K_0 *hoch genug gewählt ist,*

eine zentrale Erweiterung noch dann, wenn die Zugehörigkeit von $\mathfrak{i}$ *zu* I *nur von der Norm* $\mathfrak{i}_0$ *abhängt (ohne daß es eine Kennzeichnung der* $\mathfrak{i}_0$ *durch Kongruenzen zu geben braucht),*

überhaupt ein Normalkörper schließlich, wenn die Zugehörigkeit von Primideal-(potenz)en zu I *nur von ihrer Norm abhängt.*

Die zentralen sind unter den normalen Erweiterungen auch dadurch ausgezeichnet, daß für sie alle Klassen nach I *gegen die Substitutionen von* K/K_0 *invariant sind, während zum Normalkörper die Invarianz von* I *selbst genügt.*

Beweis. Das Kriterium für eine Abelsche Erweiterung KA geht unmittelbar aus dem Verlagerungssatz[6]) hervor: Ist $\Lambda = \mathsf{KA}$ und A ein Abelscher Körper über K_0, so gehört A in K_0 zu einer Idealgruppe I_0, die aus vollen Kongruenzklassen nach ihrem Führer $\mathfrak{m}_0$ besteht, und KA gehört dann in K zur Idealgruppe I der $\mathfrak{i}$, deren Norm in I_0 liegt. Hat umgekehrt die Idealgruppe von Λ eine mit allen Idealnormen zum Durchschnitt gebrachte Kongruenzgruppe zur Norm, und gehört zu dieser der Klassenkörper A von K_0, so ist $\Lambda = \mathsf{KA}$.

Für eine zentrale Erweiterung Λ ist die Galoisgruppe von Λ/K gegen die Substitutionen S von K elementweise invariant und dann wegen S-Operatorisomorphie mit ihr auch die Klassengruppe J/I von Λ/K, wobei J die Gruppe der unverzweigten Ideale sei. Konjugierte Ideale $\mathfrak{j}$ und $\mathfrak{j}^S$ liegen also in derselben Klasse nach I; dies gilt insbesondere für konjugierte Primideale und dann überhaupt für zwei Ideale gleicher Norm, weil deren Primidealzerlegungen durch Konjugiertenersetzung ineinander übergehen. Umgekehrt genügt schon die Feststellung, daß in I selbst mit einem Ideal $\mathfrak{i}$ auch jedes $\mathfrak{i}'$ derselben Norm liegt, um Λ als zentrale Erweiterung von K zu bestätigen: es liegt dann nämlich jeder Konjugiertenquotient $\mathfrak{j}^{S-1}$ in I (Norm $= 1$), also $\mathfrak{j}^S$ in der Klasse von $\mathfrak{j}$.

Die dem zentralen Fall gegenübergestellte Kennzeichnung der normalen Erweiterungen folgt so: Zerfällt das Primideal $\mathfrak{p}$ aus K voll in Λ, so $\mathfrak{p}^S$ in Λ^S; für $\Lambda^S = \Lambda$ liegt also $\mathfrak{p}^S$ mit $\mathfrak{p}$ in I. Allgemein dann mit $\mathfrak{i}$ auch $\mathfrak{i}^S$, aber nicht unbedingt jedes $\mathfrak{i}'$ derselben Norm, was nur für Primidealpotenzen noch keinen Unterschied macht. Umgekehrt folgt aus der Invarianz von I gegen S wegen der Eindeutigkeit des zugehörigen Klassenkörpers auch $\Lambda^S = \Lambda$.

---

[6]) H. Hasse, Ein Satz über relativ-Galoissche Zahlkörper und seine Anwendung auf relativ-Abelsche Zahlkörper, Math. Zeitschr. **31** (1930), 563. A. Scholz, Abgrenzungssätze für Kreis- und Klassenkörper, Sitz.-Ber. d. Preuß. Akad. 1931, 423.

Folgerung (Satz 7^{II}). *Innerhalb eines Normalkörpers* K/K_0 *gehört zum Zentrum seiner Galoisgruppe der kleinste Unterkörper* Z, *über dem* K *noch Klassenkörper ist und eine Idealgruppe hat, die mit einem Ideal jedes Ideal der gleichen* K_0*-Norm enthält.*

Das Kriterium kennzeichnet (Satz 7^{III}) den in einem normalen Klassenkörper Λ von K mit der Idealgruppe I enthaltenen *Geschlechterklassenkörper* und *zentralen Klassenkörper* so: *Sind* H *und* N *deren Idealgruppen innerhalb der Gruppe* J *der in* Λ/K *unverzweigten Ideale*, womit einander $J > H > N > I$ mit endlichen Indizes j, k, l enthalten, und sind J_0, $H_{(0)}$, $N_{(0)}$, I_0 deren Normen in K_0, so entsteht $N = IJ^{s-1}$ aus I durch Adjunktion aller j^{s-1}; es wird dann $N_{(0)} = I_0$ und N die Gruppe *aller* Ideale mit dieser Norm. Und $H_{(0)}$ ist die engste I_0 enthaltende Gruppe, die als Durchschnitt von J_0 mit einer Kongruenzgruppe in K_0 darstellbar ist (aus den K-Normen einer K_0-Kongruenzgruppe besteht).

Satz 1 folgt hieraus für $\Lambda = \overline{K}$: Es besteht hier I aus allen Hauptidealen von K; deren Normen bilden aber, wie behauptet, die Gruppe (N_0) der aus den Zahlnormen erzeugten Ideale, und es hat die Idealgruppe N des zentralen Klk.s K^* die in Satz 1 genannte Bedeutung.

Der Geschlechterklk. hat eine Idealgruppe H, deren Norm $H_{(0)} = [J_0, A_0]$ der Durchschnitt der Idealnormen mit der Idealgruppe A_0 des Abelschen Teilkörpers $(\overline{K})^0$ von $\overline{K}$ ist, die mit allen Zahlnormen sicher alle Normenreste nach ihrem Führer $\mathfrak{f}^0$ enthält. Satz 1 behauptet nun, daß $H_{(0)}$ die Idealgruppe der totalen Normenreste wird. Hierin liegt zuerst die Behauptung, daß jeder totale Normenrest eine Idealnorm ist. Idealnorm ist aber bereits eine Zahl μ_0, die Normenrest mod μ_0 selbst ist, die also $\mu_0 = N(\mu)\,\iota$ mit einem $\iota \equiv 1 \bmod \mu_0$ darstellbar ist; denn mit $\mu_0\iota^{-1}$ ist wegen $(\mu_0, \iota) = 1$ auch μ_0 Idealnorm.

Die restliche Behauptung ist, daß die Normenreste mod $\mathfrak{f}^0$, soweit Idealnormen, schon totale Normenreste sind. Andernfalls gäbe es nämlich von $\mathfrak{f}^0$ ein Vielfaches $\mathfrak{m}_0$, dessen Normenreste mit J_0 einen feineren Durchschnitt M_0 als $H_{(0)}$ hätten, und es gehörte zu M_0 (zur Idealgruppe M mit der Norm M_0) eine $\overline{K}^0$ echt enthaltende in $\overline{K}^*$ liegende Abelsche Erweiterung von K. Damit ist Satz 1 bewiesen.

Um Satz 2 zu beweisen, setzen wir Λ als Strahlklassenkörper nach einem noch festzulegenden Modul t an, der jedenfalls unverzweigt sein soll. Die Normgruppe von N und I wird hier die Idealgruppe $(N_0(t))$ der t-Strahlnormen, die von H aber die Gruppe $(H_0(t))$ der totalen t-Strahlnormenreste; dies wieder, weil sie wie oben der Durchschnitt von J_0 mit einer Kongruenzgruppe in K_0 ist, es aber keine feinere Gruppe dieser Art gibt, die zugleich alle t-Strahlnormen enthält. Dies ergibt erst einmal Isomorphie der Gruppe $\mathfrak{M}$ von $\Lambda/\Gamma A$ mit dem t-Idealknoten. Unser Ziel wird nun sein, t unverzweigt so zu wählen (Satz 9), daß der t-Idealknoten zum t-Zahlknoten isomorph wird; dann brauchen wir nur noch die erste Aussage von Satz 5 zu beweisen oder stattdessen

Satz 8. *Für unverzweigtes (invariantes)* t *und jede unendliche Primstelle bestehen* $H_0(t)$ *und* $N_0(t)$ *einfach aus den totalen Normenresten und Normen, die* $\equiv 1 \bmod t$ *sind.*

Hieraus folgt nämlich die Isomorphie des t-Knotens mit dem 1-Knoten deshalb, weil Normenreste mod t und Normen, und darum auch die Normenreste nach jedem Modul $t\mathfrak{m}$, dieselben Restklassen der multiplikativen[7]) Restklassengruppe mod t durchlaufen.

Nun der Beweis von Satz 8! Klar ist, daß eine Norm $N(\alpha) \equiv 1 \bmod t$, wenn $\alpha \equiv 1$, und daß dasselbe für einen Normenrest mod t gilt, also für ein $N(\alpha)\,\tau$ mit $\tau \equiv 1 \bmod t$, und darum auch für jeden totalen t-Normenrest. Es bleibt zu zeigen, daß hier auch die Umkehrung gilt. Zuerst einmal gilt sie, wenn für die Normen, so auch für die Normen-

[7]) Vgl. H. Hasse, Zahlbericht **Ia** § 3 (Definition) und **II** § 7, 3 (Auswirkung).

reste: Ist nämlich γ_0 ein Normenrest mod $\mathfrak{m}_0 = \mathfrak{t}\mathfrak{m}$, also $\gamma_0 = N(\gamma)\mu_0$ mit $\mu_0 \equiv 1 \bmod \mathfrak{m}_0$, und dabei $\gamma_0 \equiv 1 \bmod \mathfrak{t}$, so ist $\gamma_0 \mu_0^{-1} = N(\gamma) \equiv 1 \bmod \mathfrak{t}$, also $= N(\tau)$ mit einem $\tau \equiv 1 \bmod \mathfrak{t}$, falls Satz 8 für Normen richtig ist. Es wird dann $\gamma_0 = N(\tau)\mu_0$, somit t-Normenrest mod $\mathfrak{m}_0$ und, wenn eine solche Beziehung für alle (durch t teilbaren) $\mathfrak{m}_0$ gilt, auch totaler t-Strahlnormenrest.

Es bleibt also zu beweisen: Ist $\alpha_0 = N(\alpha) \equiv 1 \bmod \mathfrak{t}$ und t unverzweigt, wegen seiner Invarianz also ein Ideal [Stelle] in K_0, so ist $\alpha_0 = N(\tau)$ mit $\tau \equiv 1$ (t) darstellbar. [Für verzweigte unendliche Primstellen ist nichts zu beweisen.] Der Beweis gelingt nun so, daß man $\mathfrak{t} = \Pi \mathfrak{q}_0$ in seine Primärfaktoren zerlegt und für diese zeigt:

Ist $N(\alpha) \equiv 1 \bmod \mathfrak{q}_0$, *so ist* $\alpha \equiv \Pi \varrho^{S-1}$ *als Produkt von Quotienten konjugierter Reste* (*als „Kommutatorrest"*) *darstellbar.* Wählt man dann nämlich für $\mathfrak{t} = \mathfrak{q}_0\mathfrak{r}$ alle $\varrho \equiv 1 \bmod \mathfrak{r}$, und setzt $\alpha \Pi \varrho^{1-S} = \varkappa$, so wird $\alpha_0 = N(\varkappa)$ mit $\varkappa \equiv 1(\mathfrak{q}_0), \equiv \alpha(\mathfrak{r})$. Dies für alle Primärteiler $\mathfrak{q}_0$ von t nacheinander ausgeführt, ergibt ein $\tau \equiv 1 \bmod \mathfrak{t}$ mit $N(\tau) = \alpha_0$.

Fehlt noch der Nachweis, daß modulo einer in K unverzweigten Primidealpotenz oder unendlichen Primstelle $\mathfrak{q}_0$ jeder Rest mit der Norm 1 ein Kommutatorrest ist. Sei nun $\mathfrak{q}_0 = \Pi \mathfrak{q}^{S_i}$ die Primärzerlegung von $\mathfrak{q}_0$ in K, wobei S_i in der Gruppe von K ein rechtsseitiges Restsystem mod $\{Q\}$, der Zerlegungsgruppe von $\mathfrak{q}$ durchläuft, und $\mathrm{R} = \varrho_1, \ldots, \varrho_r, \ldots, \varrho_{rs}$ ein solches teilerfremdes Restsystem mod $\mathfrak{q}$, das $\equiv 1 \bmod \mathfrak{q}_0\mathfrak{q}^{-1}$ ist [für unendliches $\mathfrak{q}_0$ bestehend aus 1 und einem $\iota \equiv -1(\mathfrak{q}), \equiv +1$ sonst], dabei $\mathrm{R}_0 = \varrho_1, \ldots, \varrho_r$ das Teilsystem der rationalen (in K_0 liegenden) Reste mod $\mathfrak{q}$, so ergibt das direkte Produkt der R^{S_i} alle teilerfremden Reste mod $\mathfrak{q}_0$, unter denen $\prod_i \varrho_1^{S_i}, \ldots, \prod_i \varrho_r^{S_i}$ die rationalen sind (wegen $\varrho_a^{S_i} \equiv 1 \bmod \mathfrak{q}^{S_j}$ bei $j \neq i$). Jeder prime Rest ϱ ist also

$$\varrho \equiv \Pi \sigma_i^{S_i} = \sigma \Pi \sigma_i^{S_i - 1} \bmod \mathfrak{q}_0 \quad \text{mit} \quad \sigma = \Pi \sigma_i$$

und irgendwelchen σ_i aus R darstellbar, und es gilt dann $N(\varrho) \equiv N(\sigma) \bmod \mathfrak{q}_0$. Um also zu zeigen, daß ein ϱ mit $N(\varrho) \equiv 1$ Kommutatorrest mod $\mathfrak{q}_0$ ist, braucht man dasselbe nur für die σ oder allgemein für R zu zeigen. Was für $Q = 1$, insbesondere unendliches $\mathfrak{q}_0$ klar ist und sonst zu zeigen übrig läßt: daß mod $\mathfrak{q}$ jeder Rest mit der Norm 1 ein $(Q-1)$-ter Potenzrest ist. Dies gelingt durch Abzählung: Wegen der Unverzweigtheit von $\mathfrak{q}$ sind unter den rs teilerfremden Resten mod $\mathfrak{q}$ die r rationalen sämtlich Normenreste mod $\mathfrak{q}$, und daher gibt es s Reste der Norm 1. Zu diesen gehören jedenfalls die $(Q-1)$-ten Potenzreste, und das sind bereits s Reste; denn bildet man ϱ^{Q-1} für alle ϱ aus R, so wird $\varrho^{Q-1} \equiv 1$ nur für ϱ_1 bis ϱ_r. Also ist jeder Rest der Norm 1 ein Kommutatorrest.

In R ist bei der Rechnung mod $\mathfrak{q}$ gleichgültig, ob man die Norm nur bis zum Zerlegungskörper von $\mathfrak{q}$ bildet oder bis K^0, weil durch die Wahl von R für S außerhalb $\{Q\}$ die weiteren Konjugierten $\varrho^S \equiv 1(\mathfrak{q})$ werden. Ist $\mathfrak{q}$ Primideal, so wird R zyklisch und $\varrho^{Q-1} \equiv \varrho^r$, wenn Q die Frobenius-Substitution von $\mathfrak{q}$, was die Abzählung oben vereinfacht.

Damit ist Satz 8 und die in Satz 5 behauptete Isomorphie bewiesen, und es läßt sich jetzt Satz 2 so gewinnen, daß man zeigt:

Satz 9. *Es gibt in* K_0 *ein quadratfreies in* K *unverzweigtes Ideal* t, *für das jede Einheit in* K_0, *die totaler* t-*Strahlnormenrest ist, zugleich* t-*Strahlnorm ist. Die im Strahlklassenkörper mod* t *von* K *enthaltene Knotung* $\overline{\mathsf{K}}^*(\mathfrak{t})/\overline{\mathsf{K}}^0(\mathfrak{t})$ *hat eine zum Knoten von* K *isomorphe Relativgruppe.*

Wir werden dabei, wenn n der Grad von K/K_0 ist, das Ideal t so wählen — und das ist, wie sich zeigen wird, auf unendlichfache Weise möglich — daß in K_0 *jede Einheit, die* $\equiv 1$ *mod* t, *bereits eine n-te Potenz ist.*

Das gewünschte Ziel wird dann erreicht: Ist E_0 die Einheitengruppe von K_0 und $\mathrm{E}_0(\mathfrak{t})$ die Untergruppe der Einheiten, die $\equiv 1 \bmod \mathfrak{t}$, so gilt allgemein

$$(1) \qquad \mathrm{E}_0(\mathfrak{t}) > [\mathrm{E}_0, \mathrm{H}_0(\mathfrak{t})] > [\mathrm{E}_0, \mathrm{N}_0(\mathfrak{t})] > [\mathrm{E}_0(\mathfrak{t}), \mathrm{E}_0^n],$$

letztes wegen Satz 8, und zwar gilt hier Gleichheit sogar für die äußeren Gruppen, die Satz 9 nur für die mittleren Gruppen fordert. Der Einheiten-t-Knoten schrumpft also zur Identität zusammen; demnach ist der Ideal-t-Knoten zum Zahl-t-Knoten isomorph:

$$(2) \qquad (H_0(t))/(N_0(t)) \cong H_0(t)/N_0(t) \simeq H_0/N_0,$$

letztes nach Satz 5. Links steht hier aber die Norm der Klassengruppe $H(t)/N(t)$ des zentralen über dem Geschlechterklassenkörper mod t von K.

Die passende Wahl von t gelingt nun so, daß *unter den Einheiten schon jeder n-te Potenzrest mod* t *eine n-te Potenz wird*: Seien ε_1 bis ε_r die Fundamentaleinheiten von K_0 und $\varepsilon_0 = \zeta_m$ seine primitivste Einheitswurzel (m ihre Ordnung). Dann ist der Körper

$$M = K_0\left(\sqrt[n]{\varepsilon_0} = \zeta_{mn},\ \sqrt[n]{\varepsilon_1}, \ldots, \sqrt[n]{\varepsilon_r}\right)$$

über dem Körper $K_n = K_0(\zeta_n)$ das direkte Produkt der Körper $M_i = K_n\left(\sqrt[n]{\varepsilon_i}\right)$ von den Graden (m, n) für $i = 0$ und n für $i > 0$. Sonst müßte nämlich eine die Gruppe $\{E_0, \zeta_n\}$ echt enthaltende Untergruppe von $\sqrt[n]{E_0}$ bereits in K_n liegen. Liegt aber für irgendeinen Primteiler l von n die l-te Wurzel η einer K_0-Einheit in K_n, so liegt ζ_l in K_0, weil K_n/K_0 Abelsch, und η in einem Unterkörper von K_n, der wegen $\mathfrak{d}_{K_0}(\eta) \mid l \mid m$ nur der Körper $K_0(\zeta_{ml})$ sein kann, d. h. $\eta = \zeta_{ml}^a\, \eta_0$ mit η_0 in K_0.

Ist nun Z_i das Produkt aller M_j außer M_i, also $M_i Z_i = M$, so ist Z_i Zerlegungskörper einer unendlichen Schar von Primidealen $\mathfrak{q}_i$ aus K_0. Jedes Produkt $\mathfrak{t} = \mathfrak{q}_0 \mathfrak{q}_1 \cdots \mathfrak{q}_r$ hat dann die Eigenschaft, daß eine Einheit $\zeta_m^{a_0} \varepsilon_1^{a_1} \cdots \varepsilon_r^{a_r}$ nur dann n-ter Potenzrest mod t ist, wenn $(m, n) \mid a_0$ und sonst $n \mid a_i$, d. h. wenn sie wie auch $\zeta_m^{(m,n)} = \zeta_m^{mx+ny}$ eine n-te Potenz ist; denn weil $\mathfrak{q}_i$ in Z_i voll zerfällt, sind außer c_i alle ε_j $(j = 0, \ldots, r)$ n-te Potenzreste für $\mathfrak{q}_i$, während von ε_i, weil $\mathfrak{q}_i$ von Z_i nach Z, somit auch in M_i unzerfallen bleibt, für $i = 0$ erst die (m, n)-te, sonst die n-te Potenz ein n-ter Potenzrest mod $\mathfrak{q}_i$ wird; dies liefert die Teilbarkeitsaussage für a_i. An t darf hierbei jede Teilerfremdheitsforderung gestellt werden, und es ist Satz 2 mit Satz 9 bewiesen.

Bemerkung. Es genügte hier, statt des vollen Strahlklassenkörpers $\bar{K}(t)$ mod t den Klassenkörper $\bar{K}^n(t)$ zur Idealgruppe der n-ten Potenzreste mod t heranzuziehen und dann die entsprechenden Idealgruppen $H^n(t)$ und $N^n(t)$ zu bilden, deren Normen aus den n-ten Potenzresten mod t unter den totalen Normenresten und Normen bestehen. Wieder sind die Faktorgruppen $H_0^n(t)/N_0^n(t)$ und $H^n(t)/N^n(t)$ zum Knoten isomorph. Es läßt sich ferner $\bar{K}^n(t) = \bar{K}(\mathfrak{d})$ als maximaler Klassenkörper von K seiner Differente $\mathfrak{d}$ erklären, dies wegen der erzielten Quadratfreiheit des Führers. Mit der Differente rechnet sich in diesem Fall am einfachsten, weil $\mathfrak{d}(K'/K_0) = \mathfrak{d}(K/K_0) \cdot \mathfrak{d}(K'/K)$, und man erhält eine feinere Gliederung der einfach (= gradfremd) verzweigten Klassenkörper von K und ihrer zentralen Unterkörper, wenn man neben den Strahlklassenkörpern mod $\mathfrak{t} = \Pi \mathfrak{q}_i$ ($\mathfrak{q}_i$ Primideal in K_0) auch *Differentenklassenkörper* zu jedem $\mathfrak{d}$ mit echt gebrochenen Exponenten,

$$(3) \qquad \mathfrak{d} = \Pi \mathfrak{q}_i^{c_i}, \quad c_i = 1 - \frac{1}{n_i}$$

(oben waren alle $n_i = n$) betrachtet. Man erhält dann die wörtliche Übertragung der den Knoten angehenden Begriffe vom Strahl auf die Differente, indem man als „Differentenkongruenz" definiert[8]):

$$(4) \qquad \alpha \equiv 1 \ mod\, \mathfrak{d} \ \text{ mit } \mathfrak{d} \text{ aus (3) heiße: } \alpha \equiv \xi_i^{n_i}(\mathfrak{q}_i) \ \text{ mit } (\alpha, \mathfrak{d}) = 1.$$

Ferner sei $\alpha \equiv \beta \ mod\, \mathfrak{d}$ durch $\alpha\beta^{-1} \equiv 1$ erklärt. Die Kongruenz (4) schließt $\alpha \equiv 1 \ mod\, \mathfrak{d}'$ für solche $\mathfrak{d}' \mid \mathfrak{d}$ ein, die $n_i' \mid n_i$ im Exponenten haben. Der Differentenkörper *mod* $\mathfrak{d}$ kann ein solches $\mathfrak{d}'$ als Differente haben wie auch der Strahlklassenkörper mod t einen Teiler von t als Führer. Ist $\mathfrak{d}_0$ die Differente von K_0 und $(\mathfrak{d}, \mathfrak{d}_0) = 1$, so ist der $\mathfrak{d}$-Knoten $H_0(\mathfrak{d})/N_0(\mathfrak{d})$ zum 1-Knoten isomorph; im andern Fall wird man die in Satz 2 noch nicht erfaßten zentralen Körpererweiterungen erhalten.

---

[8]) Vgl. „m-kongruent" in Hasses Zahlbericht **II**, S. 41!

Satz 3 und 4 folgen jetzt unter Anwendung von F., Satz 5 auf die Galoisgruppe $\mathfrak{L}$ einer die Forderungen des Satzes 2 erfüllenden zentralen Erweiterung Λ von Γ: Die zum Knoten K isomorphe Gruppe $\mathfrak{M}$ von $\Lambda/\Gamma\Lambda^0$ ist danach homomorph zum Darstellungsmultiplikator von $\mathfrak{G}$, wie Satz 3 besagt. Für Satz 4 halte man sich dabei an Fig. 3 in F., Satz 5. Es ist hier die Aufgabe, den Knotungsmultiplikator $\mathfrak{M}$ „unmittelbar an die Gruppe $\mathfrak{G}$ anzusetzen" und so eine dem Knoten entsprechende Knotung von Γ unter Auslassung der Abelschen Erweiterung $\Gamma A/\Gamma$ ($A = \Lambda^0$) mit der Gruppe A zu finden. Dazu bedarf es einer bei genügender Geschmeidigkeit von Γ ausführbaren absolut Abelschen Adjunktion $\Gamma A(\beta)$, deren Relativgruppe $\mathfrak{B}$ zu $\mathfrak{M}$ isomorph und mit $\mathfrak{A}$ in der gleichen Weise wie $\mathfrak{M}$ verknüpft ist. (Dabei kann der Abelsche Körper $A(\beta)$ unter Weglassung direkter Adjunktionen auf eine in ihm enthaltene Verlängerung, also ein Produkt zyklischer Verlängerungen, reduziert werden, da auch in $\mathfrak{A} \cup \mathfrak{M}$ die direkten Teile von $\mathfrak{M}$ undurchkreuzt bleiben können.) Durch Identifizierung der auf diese Weise einander entsprechenden Elemente von $\mathfrak{A} \cup \mathfrak{B}$ und $\mathfrak{A} \cup \mathfrak{M}$ erhält man dann die Gruppe einer dem Knoten entsprechenden Knotung N von Γ (in Fig. 3 mit Relativgruppe $\mathfrak{N} \cong K$ und absoluter Gruppe $\mathfrak{K}$; hier vertauscht man besser die Bezeichnungen $\mathfrak{N}$ und $\mathfrak{K}$). — Die Erweiterbarkeit von A zu einem $A(\beta)$ ist dabei wirklich notwendig; denn in ΛN ist eine solche Abelsche Erweiterung enthalten; diese ist aber nur dann trivialerweise konstruierbar, nämlich ein direktes Produkt $A \times B$, wenn Λ selbst Abelsche Erweiterung einer Knotung, also $\Lambda = NA$ darstellbar ist. Zur Gewinnung einer Knotung N aus dem Körper Λ vgl. die Beispiele $a > 0$ auf S. 229.

Die Durchkreuzung mit allen Abelschen Erweiterungen von Γ, deren Relativgruppe zu $\mathfrak{M}$ isomorph ist, liefert alle mit N verwandten Knotungen von Γ, und zwar durchlaufen deren Galoisgruppen wirklich alle mit $\mathfrak{N}$ verwandten Gruppentypen, weil jede Verbindung der Gruppe $\mathfrak{G}$ mit einer zu $\mathfrak{M}$ isomorphen Gruppe infolge der Geschmeidigkeitsvoraussetzung durch Körper realisierbar ist und so zur Durchkreuzung von $\mathfrak{N}$ herangezogen werden kann. Damit ist Satz 4 bewiesen. Die Kennzeichnung der verschiedenen Typen der Klasse von N durch Wiederverzweigung in Γ verzweigter Ideale vgl. S. 232ff.

Um Satz 5 vollständig zu beweisen, beachte man, daß Satz 3 ebenfalls für jeden t-Idealknoten gilt, weil auch der zentrale Klassenkörper mod t über dem Geschlechterklassenkörper mod t eine Knotung ist, deren Relativgruppe nach F., Satz 5 zum Darstellungsmultiplikator von $\mathfrak{G}$ homomorph ist. Also besteht erst einmal eine durch die Struktur von $\mathfrak{G}$ bestimmte Schranke für alle Idealknoten, wobei weitere Beschränkungen noch durch die zahlentheoretische Beschaffenheit von K hinzukommen können. Es genügt somit zu beweisen:

A. *Es gibt eine zentrale Erweiterung* M *von* K *mit der Eigenschaft, daß jede andere zentrale Erweiterung* Λ *in* M *oder einer Abelschen Erweiterung* MA *von* M *enthalten ist.* (Für die Galoisgruppen $\mathfrak{L}$ und $\mathfrak{M}$ heißt das, daß $\mathfrak{L}$ zum Geschlecht einer Faktorgruppe von $\mathfrak{M}$ gehört, also die Ableitung $\mathfrak{L}'$ zu $\mathfrak{M}'$ und $(\mathfrak{L} \circ \mathfrak{M})'$ homomorph ist.)

B. *Ist* $\mathfrak{f}$ *der Führer von* M/K, *so ist der* $\mathfrak{f}$*-Strahlidealknoten, der ja zur in* M *enthaltenen Knotung gehört, zum* $\mathfrak{f}$*-Strahlzahlknoten isomorph, und alle Strahlknoten von* K/K_0 *sind hierzu homomorph.*

C. *Ist* $\mathfrak{w} = \mathfrak{u}\mathfrak{v}$ *die Zerlegung eines invarianten Ideals von* K *in seinen unverzweigten und verzweigten Bestandteil, so ist der* $\mathfrak{w}$- *zum* $\mathfrak{v}$*-Strahlknoten isomorph, insbesondere für* $\mathfrak{w} = \mathfrak{f}$ *der* $\mathfrak{v}$*-Strahlknoten maximal.*

Die Behauptung von Satz 5, daß die in Λ/K enthaltene Knotung bei in K unverzweigtem Führer $\mathfrak{f}$ eine zum 1-Knoten homomorphe Relativgruppe hat, folgt dann so, daß der $\mathfrak{f}$-Idealknoten zum $\mathfrak{f}$-Zahlknoten homomorph und dieser zum 1-Knoten isomorph ist, und die unmittelbare Knotbarkeit bei Geschmeidigkeit von K wie oben.

Auf Grund von A. und C. (auch schon E., s. u.) läßt sich B. durch die leichter zu beweisende Behauptung ersetzen:

D. *Zu invariantem, insbesondere verzweigtem* $\mathfrak{v}$ *gibt es ein unverzweigtes* $\mathfrak{t}$, *für das der* $\mathfrak{vt}$*-Idealknoten zum* $\mathfrak{vt}$*-Zahlknoten und damit zum* $\mathfrak{v}$*-Knoten isomorph ist.*

Dann ist nämlich, wenn in den obigen Bezeichnungen $\mathfrak{f} = \mathfrak{uv}$ der Führer von $\mathfrak{M}$ ist, schon sein unverzweigter Teiler $\mathfrak{u}$ eines der Ideale $\mathfrak{t}$, die D. erfüllen, da bei bloßer Homomorphie des $\mathfrak{uv}$-Idealknotens zum $\mathfrak{v}$-Knoten der Strahlklassenkörper $\bmod \mathfrak{f} = \mathfrak{uv}$ eine schwächere Knotung hätte als der $\bmod \mathfrak{tv}$, und es ist der $\mathfrak{v}$-Knoten wirklich maximaler Strahlknoten. D. schließt also die letzte Behauptung von C. mit ein.

Von den Behauptungen A., C., D. beweisen wir zuerst C. (ohne die an D. überwiesene Behauptung über $\mathfrak{w} = \mathfrak{f}$) in der Satz 8 entsprechenden Form:

E. *Eine Zahl* α_0 *ist* (*totaler*) $\mathfrak{w}$*-Strahlnorm*(*enrest*), *wenn sie* (*totaler*) $\mathfrak{v}$*-Strahlnorm*(*enrest*) *ist und überdies* $\alpha_0 \equiv 1$ *mod* $\mathfrak{u}$ *gilt.* (Wie in C. sei $\mathfrak{w} = \mathfrak{uv}$ invariant und $\mathfrak{u}$ unverzweigt.)

Mit der Bemerkung, daß Normen und Normenreste dieselben Restklassen der multiplikativen Restklassengruppe durchlaufen, folgt hieraus nämlich wieder

$$H_0(\mathfrak{w})/N_0(\mathfrak{w}) = H_0(\mathfrak{uv})/N_0(\mathfrak{uv}) \simeq H_0(\mathfrak{v})/N_0(\mathfrak{v}).$$

E. beweist man wie Satz 8: Ist $\alpha_0 = N(\alpha) \equiv 1 \bmod \mathfrak{w}$ und dabei $\alpha \equiv 1 \bmod \mathfrak{v}$, wie vorausgesetzt, so ist $\alpha \bmod \mathfrak{u}$ nach dem Beweis von Satz 8 als Kommutatorrest $\alpha \equiv \Pi\gamma^{s-1}$ darstellbar. Wählt man nun ein $\beta \equiv \gamma \bmod \mathfrak{u}$, $\equiv 1 \bmod \mathfrak{v}$ und setzt $\alpha\beta^{1-s} = \tau$, so wird $\tau \equiv 1 \bmod \mathfrak{w}$ und $N(\tau) = \alpha_0$. Also ist α_0 auch $\mathfrak{w}$-Strahlnorm. Für Normenreste $\alpha_0 = N(\alpha)\mu$ mit $\mu \equiv 1\ (\mathfrak{m}\mathfrak{w})$ verfahre man wieder entsprechend mit $\alpha_0\mu^{-1} = N(\alpha)$.

D. wird nun von einem Teil der $\mathfrak{t}$ aus Satz 9 sicher erfüllt: Ist a die Anzahl der teilerfremden Reste $\bmod \mathfrak{v}$ in K, so wähle man $\mathfrak{t}$ so aus, daß die Strahleinheiten $\eta_0 \equiv 1 \bmod \mathfrak{t}$ in K_0 nicht nur n-te, sondern an-te Potenzen werden, also $\eta_0 = \varepsilon_0^{an} = N(\varepsilon_0^a)$ mit $\varepsilon_0^a \equiv 1 \bmod \mathfrak{v}$ ausfallen und damit $\mathfrak{tv}$-Strahlnormen werden. Zu den $\eta_0 \equiv 1\ (\mathfrak{t})$ gehören aber vor allem die totalen $\mathfrak{tv}$-Strahlnormenreste unter den Einheiten; die Einheiten sind also $\mathfrak{tv}$-knotenfrei, und daher ist der $\mathfrak{tv}$-Idealknoten isomorph zum $\mathfrak{tv}$-Zahlknoten.

(Für unverzweigtes $\mathfrak{v}$ reicht wie bei Satz 9 jedes $\mathfrak{t}$, dessen Strahleinheiten n-te Potenzen sind, weil dann die $\eta_0 \equiv 1\ (\mathfrak{tv})$ schon immer Normen und damit $\mathfrak{tv}$-Strahlnormen sind.)

A. folgt unabhängig von C., D. aus der oben festgestellten Beschränkung aller Idealknoten durch den Darstellungsmultiplikator von $\mathfrak{G}$. Danach gibt es sicher ein $\mathfrak{f}$, dessen Idealknoten maximale Ausdehnung hat. Allgemein ist aber für $\mathfrak{v} \mid \mathfrak{w}$ der $\mathfrak{v}$- zum $\mathfrak{w}$-Idealknoten homomorph; denn $\overline{K}^*(\mathfrak{w})$, der zentrale Klassenkörper $\bmod \mathfrak{w}$, enthält die Abelsche Erweiterung $\overline{K}^*(\mathfrak{v})\overline{K}^0(\mathfrak{w})$ von $\overline{K}^*(\mathfrak{v})$, die über $\overline{K}^0(\mathfrak{w})$ eine zur Gruppe von $\overline{K}^*(\mathfrak{v})/\overline{K}^0(\mathfrak{v})$, also zum $\mathfrak{v}$-Idealknoten isomorphe Gruppe hat. Dieser ist dann echt homomorph zum $\mathfrak{w}$-Idealknoten, wenn $\overline{K}^*(\mathfrak{w}) \neq \overline{K}^*(\mathfrak{v})\overline{K}^0(\mathfrak{w})$. Für $\mathfrak{w} = \mathfrak{fv}$ folgt daraus Homomorphie des $\mathfrak{f}$- und $\mathfrak{v}$-Idealknotens zum $\mathfrak{fv}$-Idealknoten; diese ist aber für den $\mathfrak{f}$-Idealknoten infolge seiner Maximalität eine Isomorphie, und infolgedessen ist $\overline{K}^*(\mathfrak{w})$ nur eine Abelsche Erweiterung von $\overline{K}^*(\mathfrak{f})$.

Anders dargestellt: Ist M eine in dem Sinne maximale zentrale Erweiterung von K, daß jede M enthaltende zentrale Erweiterung N eine Abelsche Erweiterung von M ist, so ist jede zentrale Erweiterung Λ von K in einer Abelschen Erweiterung von M enthalten, nämlich in $N = \Lambda M$. Besäße aber jedes zentrale M noch eine über K zentrale nicht-Abelsche Erweiterung N, so gäbe das echte Homomorphie der Gruppe jedes M/KM^0 zur Gruppe eines N/KN^0, also keine Knotenschranke.

(Gruppenisomorphie bestünde dann nur noch zwischen M/KM^0 und H/K^0H, wo H die maximale in N enthaltene Abelsche Erweiterung von M ist; was von N über H hinausragt, spaltet den Knoten auf.)

Damit sind jetzt alle Aussagen von Satz 5 bewiesen.

Bemerkung. Die Verzweigungsfremdheit von Λ/K zu K ist zugleich mit der von $\Lambda/K\Lambda^0$ zu K erreichbar, weil Teile von $K\Lambda^0/K$, in denen sich ein $\mathfrak{v}$ verzweigt, ohne sich in $\Lambda/K\Lambda^0$ weiter zu verzweigen, direkt abspaltbar sind, und daher ist zusammen mit Satz 2 erreichbare Verzweigungsfremdheit von $\Lambda/K\Lambda^0$ kennzeichnend für Galoisisomorphie zum 1-Knoten.

Satz 6 beweisen wir so, daß wir zu jeder Gruppe $\mathfrak{H}$ einen Körper K_0 aufweisen, der einen unverzweigten Oberkörper X mit der Gruppe $\mathfrak{H}$ besitzt. Ist dabei $\mathfrak{H}$ Darstellungsgruppe von $\mathfrak{G}$, so ist $\mathfrak{G}$ die Galoisgruppe eines Unterkörpers K/K_0 von X/K_0. Infolge der Unverzweigtheit von X auch über K hat K nach Satz 5 einen 1-Knoten, zu dem die Gruppe von X/K homomorph ist; umgekehrt ist aber auch der Knoten nach Satz 3 zu $\mathfrak{M}$ als dem Darstellungsmultiplikator von $\mathfrak{G}$ homomorph, also hier isomorph, wie in Satz 6 verlangt.

Die Unverzweigtheit von X/K_0 fordern wir hier, um zu verhüten, daß etwa in K/K_0 verzweigtes $\mathfrak{v}$ sich in X/K weiterverzweigt und so etwa nur $\mathfrak{v}$-Knotenisomorphie mit $\mathfrak{M}$ entsteht.

Die Konstruktion eines X/K_0 leisten wir so, daß wir $\mathfrak{H}$ in eine symmetrische Permutationsgruppe $\mathfrak{S}_p$ von Primzahlgrad p einbetten; das geht sicher für das auf die Ordnung h von $\mathfrak{H}$ folgende p. Zu $\mathfrak{S}_p$ konstruieren wir erst einmal über dem rationalen Zahlkörper eine zugehörige Galoisresolvente Σ und setzen sie dann zu ihrer Entzweigung auf einen Kummerschen Körper P auf, in dem alle in Σ Verzweigten in gleicher oder vielfacher Potenz verzweigt sind. Dann soll $P\Sigma = X$ werden. Um dabei sicher zu gehen, daß X/P unverzweigt wird, fordern wir für Σ noch Gradfremdheit der Verzweigten, d. h. also, da $p!$ der Grad von Σ ist, daß alle Diskriminantenteiler größer als p sein sollen. Dann werden nämlich alle Verzweigungen einfach, d. h. die Verzweigungsgruppen werden eins und die Trägheitsgruppen zyklisch.

Daß dann $P\Sigma/P$ unverzweigt wird, folgt so: Es sei die Primzahl q in Σ eine e-te Potenz und T der Trägheitskörper eines Primteilers $\mathfrak{q}$ von q in Σ, dabei Σ/T vom Grade e, ferner $\mathfrak{r}$ ein Primteiler von q in P, dabei $\mathfrak{U}$ die Untergruppe der Ordnung e seiner Trägheitsgruppe und Y der zugehörige Unterkörper von P. Dann hat ein gemeinsamer Primteiler von $\mathfrak{q}$ und $\mathfrak{r}$ in $P\Sigma/Y$ einen YT enthaltenden Trägheitskörper, also eine in der Gruppe von $P\Sigma/YT$, einer Abelschen Gruppe vom Typ (e, e), liegende Trägheitsgruppe, die dann nur eine zyklische Gruppe der Ordnung e sein kann. Dann kann aber $\mathfrak{r}$, das innerhalb P/Y bereits von e-ter Ordnung verzweigt ist, in $P\Sigma$ nur noch in verschiedene Faktoren zerfallen. Also ist $P\Sigma/P$ unverzweigt.

Wir treffen jetzt die Wahl von P und Σ nach den genannten Bedingungen. Hier ist Σ als Resolventenkörper einer Gleichung p-ten Grades mit symmetrischer Gruppe erklärbar, etwa

$$\Sigma: \qquad x^p - aqx - q = 0.$$

Dabei sei q die auf p folgende Primzahl, die schon die Irreduzibilität der Gleichung sichert. Über a werden wir so verfügen, daß die Gleichungsdiskriminante

$$D = \pm (p-1)^{p-1} a^p q^p \pm p^p q^{p-1}$$

zu $p!$ prim wird und einen Primfaktor l besitzt, der in D genau in erster Potenz aufgeht. Durch die letzte Maßnahme wird erreicht[9]), daß die Gleichungsgruppe die symmetrische

[9]) A. Scholz, Aufgabe 171, Lösung 4, Jahresber. D. M. V. **45** (1935), *42*.

ist. Sicher ist nun $(D, p!) = 1$, wenn a durch das Produkt c der Primzahlen unter p, aber nicht durch p selbst teilbar ist. Entweder hat dann D für $a = c$ einen Einzelprimteiler l und S die gewünschte Gestalt. Sonst aber hat $D = \pm q^{p-1}(Aq + p^p)$ wenigstens noch einen von q verschiedenen Primteiler l, der in einer neuen Gleichungsdiskriminante D' in erster Potenz auftritt, indem man jetzt $a = c(1 + l)$ oder $= c(1 - l)$, nur $\not\equiv 0 \bmod p$ wählt. Es wird dann

$$D' - D = (p-1)^{p-1} c^p (\pm pl + kl^2) q^p \equiv 0\ (l),\ \not\equiv 0\ (l^2).$$

Für eines der genannten a erhält man also sicher einen passenden Normalkörper Σ. Jetzt wählen wir

$$\mathsf{P} = \mathsf{P}_0\left(\zeta_{p!}, \sqrt[p!]{dz}\right).$$

Hierbei sei P_0 der rationale Zahlkörper, d das Produkt der Primteiler von D, unter denen auch alle Primteiler der Diskriminante von Σ, also alle in Σ verzweigten Primzahlen vorkommen, und z eine in $p!D$ nicht aufgehende Primzahl, die verhindern soll, daß der Körper Σ beim Aufsetzen in P hineinrutscht. Denn es ist ja möglich, daß $\mathsf{P}(\sqrt{d})$ oder $\mathsf{P}(\sqrt{-d})$ gerade den quadratischen Unterkörper von Σ liefert; für $z = 1$ lägen aber (bei $p \geqq 5$) beide Körper in P, und es wäre $\mathsf{P}\Sigma/\mathsf{P}$ nur alternierend. Insbesondere tritt das für quadratfreies D ein; dann aber genügte schon $\mathsf{P} = \mathsf{P}_0(\sqrt{2d})$ als Unterbau, wie im allgemeinen ein echter Unterkörper von obigem P genügt, um Σ zu entzweigen. Da $\mathsf{P}_0(\sqrt{D})$ aber der einzig auflösbare Teil von Σ ist, braucht nur für diesen die Teilerfremdheit mit P bestätigt zu werden, und diese Bedingung ist für den oben angegebenen Normalkörper P zusammen mit den geforderten Verzweigungen erfüllt.

Nunmehr findet man zwischen P und $\mathsf{P}\Sigma$ ein Satz 6 erfüllendes Körperpaar K_0, K, indem man in der Gruppe von $\mathsf{P}\Sigma/\mathsf{P}$ eine Untergruppe vom Typ $\mathfrak{H}$ und von dieser eine Faktorgruppe vom Typ $\mathfrak{G}$ bildet und die zugehörigen Unterkörper bestimmt. Obendrein ist gezeigt, daß jede endliche Gruppe als Galoisgruppe eines unverzweigten Relativkörpers auftritt.

Zur Erläuterung von Satz 2 und 4 bringen wir einige Beispiele von Körpern mit Vierergruppe und einem Knoten der Ordnung 2, die teils direkt eine Knotung zulassen, sich also zu einem Körper mit Dieder- oder Quaternionengruppe erweitern lassen, teils aber erst ein quadratisches Stück Geschlechterklassenkörper adjungieren müssen, um einer nicht-Abelschen zentralen Erweiterung fähig zu sein, die nach Satz 2 hier auch für „sprödes“ K existieren muß.

Als Grundkörper K_0 wählen wir durchweg den rationalen Zahlkörper, und den zu erweiternden biquadratischen Zahlkörper $\mathsf{K} = \mathsf{K}_0(\sqrt{D}, \sqrt{D'})$ so, daß er nicht das Produkt verzweigungsfremder quadratischer Körper wird, und dabei D und D' quadratfrei von der Form $4n + 1$. Ist also, wenn alle Zerlegungen in vorzeichenbehaftete Faktoren der Form $4n + 1$ vorgenommen werden, $D = rs$ und $D' = rt$ mit $(s, t) = 1$, so ist $\mathsf{K}_0(\sqrt{st})$ der dritte in K enthaltene Körper, und die obige Forderung lautet $r, s, t > 1$. Sind r_i, s_j, t_k die Primfaktoren von r, s, t, so ist der Körper

$$\tilde{\mathsf{K}}^0 = \mathsf{K}_0(\sqrt{r_1}, \ldots, \sqrt{r_i}, \ldots\ldots, \sqrt{s_j}, \ldots\ldots, \sqrt{t_k}, \ldots) = \Pi\, \mathsf{P}_i \Sigma_j \mathsf{T}_k$$

der volle Geschlechterklassenkörper mod -1 von K, wo -1 die unendliche rationale Primstelle bezeichnet, die hier Führer wird, wenn eins der r_i, s_j, t_k negativ bei reellem K ist, während sonst $\tilde{\mathsf{K}}^0 = \overline{\mathsf{K}}^0$. Der für unsere Betrachtung wesentliche Teil von $\tilde{\mathsf{K}}^0$ wird $\Lambda = \mathsf{K}_0(\sqrt{r}, \sqrt{s}, \sqrt{t}) = \mathsf{P}\Sigma\mathsf{T}$ werden.

Die Lage der Trägheitsgruppen, die ja bei rationalem Grundkörper stets die ganze Galoisgruppe erzeugen, ist, wenn man von der zur Erzeugung überflüssigen unendlichen Primstelle hier ganz absieht, dabei folgende: In Λ haben noch wie in K die Primteiler der r, s, t gemeinsame Trägheitsgruppen $\{R\}, \{S\}, \{T\}$, während sie in $\widetilde{\mathsf{K}}^0$ je eine besondere Trägheitsgruppe $\{R_i\}, \{S_j\}, \{T_k\}$ besitzen. Während sie aber in K noch abhängig sind ($RST = 1$), bilden sie in Λ schon wie in $\widetilde{\mathsf{K}}^0$ eine Basis für die Galoisgruppe, und es wird Λ das (über K kleinste) Produkt verzweigungsfremder zyklischer Körper.

Unsere Untersuchung gilt nun dem Fall, daß K einen Knoten der Ordnung 2 hat. Hier ist bereits $\widetilde{\mathsf{K}}^*$ eine Satz 2 erfüllende zentrale Erweiterung von K, also $\widetilde{\mathsf{K}}^*/\widetilde{\mathsf{K}}^0$ vom Grade 2; denn -1 ist wie auch jedes q der Form $4n-1$ ein Satz 9 erfüllendes Ideal $\mathfrak{t}$, weil die erzeugende rationale Einheit -1 quadratischer Nichtrest für q ist. (Es hat darum auch $\overline{\mathsf{K}}^*(q)/\overline{\mathsf{K}}^0(q)$ den Grad 2, während das für $\overline{\mathsf{K}}^*/\overline{\mathsf{K}}^0$ nur der Fall ist, wenn der Knoten von K ein Idealknoten ist.)

Ist nun C die erzeugende Substitution von $\widetilde{\mathsf{K}}^*/\widetilde{\mathsf{K}}^0$, also $C^2 = 1$, so erzeugt C mit den Trägheitssubstitutionen R_i, S_j, T_k je eines Primteilers der r_i, s_j, t_k zusammen die absolute Galoisgruppe $\mathfrak{G}$ von $\widetilde{\mathsf{K}}^*$, deren jedes Element sogar als geordnetes Produkt der R_i, S_j, T_k, C mit Exponenten 0, 1 darstellbar ist, und diese hat die Relationen

$$\mathfrak{G}: \quad \begin{array}{l} R_i^2 = S_j^2 = T_k^2 = 1; \quad (R_i, R_j) = (S_i, S_j) = (T_i, T_j) = 1; \\ (R_i, S_j) = (S_j, T_k) = (T_k, R_i) = C; \quad C^2 = 1; \quad (C, \mathfrak{G}) = 1. \end{array}$$

Für K kommen dazu die Relationen

$$\mathfrak{R}: \quad R_i = R_1; \quad S_j = S_1; \quad T_k = T_1; \quad R_1 S_1 T_1 = 1; \quad C = 1.$$

(Für die Gruppe $\mathfrak{L}$ von Λ fällt die vorletzte Relation fort.)

M. a. W.: Es ist $\mathfrak{R}$ die Faktorgruppe $\mathfrak{G}/\mathfrak{X}$ nach

$$\mathfrak{X} = \{R_1 R_i, S_1 S_j, T_1 T_k, R_1 S_1 T_1, C\} = \{R_i S_j T_k\}, \qquad i, j, k = 1, 2, \ldots$$

Von den angegebenen Relationen, die uns alle zusammen für $\mathfrak{R}$ schon bekannt sind, folgen die für $\mathfrak{G}$ so: $R_i^2 = 1$, weil r_i in $\widetilde{\mathsf{K}}^*/\widetilde{\mathsf{K}}^0$ nicht mehr verzweigt ist, und $(R_i, R_j) = 1$, weil ein Kommutator zweier Elemente nur von deren Restklassen nach dem Zentrum abhängt, in dem sicher $\mathfrak{X}$ liegt, da $\mathfrak{G}$ eine zentrale Aufspaltung von $\mathfrak{R}$ ist. Aus demselben Grunde stimmen $(R_i, S_j) = (R_i, R_i T_k)$ und $(S_j, T_k) = (R_i T_k, T_k)$ mit (R_i, T_k) überein und sind $= C$, da sonst $\mathfrak{G}$ kommutativ würde.

An Produktquadraten wird

$$(R_i S_j)^2 = R_i^2 S_j^2 \ (R_i, S_j) = C,$$
$$(R_i S_j T_k)^2 = (R_i, S_j)\,(R_i, T_k)\,(S_j, T_k) = C,$$

und darum schon $\{R_i S_j T_k\}_{i,j,k} = \mathfrak{X}$, wie oben behauptet, aber $(R_i R_j)^2 = R_i^2 R_j^2 = 1$ und daher

$$\mathfrak{Z} = \mathfrak{G}/\mathfrak{Y} \text{ mit } \mathfrak{Y} = \{R_1 R_i, S_1 S_j, T_1 T_k\}_{i,j,k}$$

bereits eine *zentrale Aufspaltung von* $\mathfrak{R}$, die mit den Relationen

$$\mathfrak{Z}: \quad R^2 = S^2 = T^2 = 1; \quad (R, S) = (R, T) = (S, T) = C; \quad C^2 = 1$$

— Indizes bei Zusammenfall der Trägheitssubstitutionen gestrichen — eine *unmittelbare Knotung von* $\mathfrak{L}$ darstellt.

$\mathfrak{Y}$ spaltet sich dabei direkt von $\mathfrak{G}$ ab, und dementsprechend zerfällt

$$\widetilde{\mathsf{K}}^* = \mathsf{Z} \times \mathsf{K}_0(\sqrt{r_2}, \ldots, \sqrt{s_2}, \ldots, \sqrt{t_2}, \ldots).$$

Z ist, falls echter Teil von K^*, nicht eindeutig bestimmt, sondern besitzt 2^v verwandte Erweiterungen von K innerhalb $\widetilde{\mathsf{K}}^*$, wo $2^v = \mathrm{Ord}\ \mathfrak{Y} = \mathrm{Grad}\ \widetilde{\mathsf{K}}^0/\Lambda$ ist: Man

erhält ein neues $\mathfrak{Y}$), wenn man in seiner Basis etwa $R_1 R_i$ durch $R_1 R_i C$ ersetzt, also die Trägheitssubstitution R_i durch ihre Konjugierte $R_i C = R_i^S = R_i^T$, was praktisch zur Durchkreuzung von Z mit $\mathsf{K}_0(\sqrt{r_i})$ führt. Dies für alle R_i, S_i, T_i mit $i > 1$ durchgeführt, ergibt eine ganze Charaktergruppe von $\mathfrak{Y}$ an Möglichkeiten.

Eine Knotung von K selbst ist nun in Z nicht enthalten; denn bei $C = (RST)^2$ ist Z/K zyklisch vom Grade 4 mit Λ als einzigem Zwischenkörper. Zu einer unmittelbaren Knotung von K bedarf es daher einer Durchkreuzung von Z mit einer zyklischen Verlängerung M von Λ, in der RST ebenfalls die Ordnung 4 hat. In dieser S. 233 erläuterten, abgekürzten Sprache hat dann M eine Gruppe $\{R, S, T\}$ der Ordnung 16 entweder mit $R^4 = S^2 = T^2 = 1$ oder entsprechend für S oder T statt R oder viertens mit $R^4 = S^4 = T^4 = 1$ bei $(RS)^2 = (ST)^2 = 1$. In der Gruppe von $\Lambda\mathsf{M}$ gehört zu $RST = 1$ jetzt eine Knotung N von K, die in den ersten drei Fällen eine Diedergruppe hat (im ersten Fall $S^2 = T^2 = 1$; $R = ST$; $R^2 = (S, T)$; $R^4 = 1$) und im vierten Fall die Quaternionengruppe (alle Trägheitssubstitutionen R, S, T von der Ordnung 4). Damit aber R als Trägheitssubstitution die Ordnung 4 haben kann, muß $\mathfrak{r}$ lauter positive Primteiler $\equiv 1 \bmod 4$ haben (Quadratsumme sein), und das reicht auch hin, damit P eine zyklische Verlängerung besitzt, die im ersten Fall (bis auf eine direkte Durchkreuzung) die ganze und im vierten eine Teildurchkreuzung leistet.

Es gibt darum, wie in der folgenden Körpertafel in erster Spalte vermerkt, keine Knotung von K, nur eine Art Diederknotung, ein Paar solcher oder alle vier Knotungstypen samt Quaternionentypus, je nachdem unter den Zahlen r, s, t keine, eine, zwei oder alle eine Quadratsumme sind. Beispiele:

a	c	r	s	t	K
4	3	5	29	109	$(\sqrt{145}, \sqrt{545})$
	2	13	17	$185 = 5 \cdot 37$	$(\sqrt{221}, \sqrt{2405})$
	1	5	13	37	$(\sqrt{65}, \sqrt{185})$
2	3	-3	13	61	$(\sqrt{-39}, \sqrt{-183})$
	2	-3	13	$205 = 5 \cdot 41$	$(\sqrt{-39}, \sqrt{-615})$
	1	-3	$65 = 5 \cdot 13$	$1037 = 17 \cdot 61$	$(\sqrt{-195}, \sqrt{-3111})$
1	3	-3	37	$469 = 7 \cdot 67$	$(\sqrt{-111}, \sqrt{-1407})$
	2	-7	29	$57 = 3 \cdot 19$	$(\sqrt{-203}, \sqrt{-399})$
	1	-11	13	$21 = 3 \cdot 7$	$(\sqrt{-143}, \sqrt{-231})$
0	3	$93 = 3 \cdot 31$	$133 = 7 \cdot 19$	$253 = 11 \cdot 23$	$(\sqrt{12369}, \sqrt{23529})$
	2	-3	$217 = 7 \cdot 31$	$253 = 11 \cdot 23$	$(\sqrt{-651}, \sqrt{-759})$
	1	$129 = 3 \cdot 43$	$209 = 11 \cdot 19$	$413 = 7 \cdot 59$	$(\sqrt{26961}, \sqrt{53277})$.

Die Anzahl a der vorhandenen Knotungstypen von K ist dabei sofort aus der Zerlegung der r, s, t ersichtlich, sobald man weiß, daß Λ eine Knotung Z vom Typus der oben definierten Gruppe $\mathfrak{Z}$ besitzt. Um dies zu entscheiden, stützen wir uns entweder auf den Richterschen Einbettungssatz[10]) (s. u.) oder untersuchen ausführlicher die maximalen unverzweigten Knotungen von Λ, deren Gruppe eine Faktorgruppe der Darstellungsgruppe $\mathfrak{H}$ von $\mathfrak{L}$ mit den Relationen

$$R^2 = S^2 = T^2 = (R, S)^2 = (R, T)^2 = (S, T)^2 = 1; (\mathfrak{H}', \mathfrak{H}) = 1$$

[10]) H. Richter, Über die Lösbarkeit einiger nicht-Abelscher Einbettungsprobleme, Math. Ann. **112** (1936), 72.

und der Ordnung 64 wird, und zwar ist es wegen Nichtweiterverzweigung der r, s, t gerade dieser Typus $\mathfrak{H}$. Wir haben also die Gruppen $\mathfrak{Q}$ mit $\mathfrak{Z} \prec \mathfrak{Q} \prec \mathfrak{H}$ zu studieren.[11])

Die oben in zweiter Spalte angegebene Anzahl c der Basiselemente von $\mathfrak{Q}'$ entscheidet hier die Struktur von $\mathfrak{Q}$: während $c = 3$ zu $\mathfrak{Q} = \mathfrak{H}$ führt und $c = 1$ zu $\mathfrak{Q} = \mathfrak{Z}$, wo die drei Kommutatoren zusammenfallen, müssen für $c = 2$ zwei Kommutatoren zusammenfallen, der dritte aber von ihnen unabhängig sein; hingegen darf wegen $\mathfrak{Q} \succ \mathfrak{Z}$ nicht etwa ein Kommutator verschwinden. Für $c = 2$ gibt es also drei Gruppentypen $\mathfrak{Q}$, die aber bei Vertauschung der Erzeugenden ineinander übergehen, also dieselbe Struktur haben.

Erkennbar sind die Typen $\mathfrak{Q}$ an folgendem: Es ist $\mathfrak{H}$ das relative Produkt seiner zu $T = 1$, $S = 1$ und $R = 1$ gehörigen Faktorgruppen, dreier die Körper $\mathsf{P\Sigma}$, PT und $\mathsf{\Sigma T}$ knotenden Diedergruppen. Die Knotbarkeitsbedingung für $\mathsf{P\Sigma}$ lautet hier aber[12]) [13]), daß in $\mathsf{P} = \mathsf{K}_0(\sqrt{r})$ die Primteiler von s und in $\mathsf{\Sigma} = \mathsf{K}_0(\sqrt{s})$ die von r voll zerfallen, also: daß r und s gegenseitig quadratische Reste sind. Somit ist gegenseitiger quadratischer Rest von r, s, t die Bedingung für verzweigungsfremde und damit auch für unverzweigte Einbettung von Λ in einen Körper mit der Gruppe $\mathfrak{H}$. (Als quadratischer Rest für -1 zählt eine positive Zahl!)

Für den Typus $\mathfrak{Q}$ mit $(R, S) \neq (R, T) = (S, T)$ gelten die Bedingungen, daß r und s gegenseitig quadratische Reste sind sowie rs und t; dies, damit die Aufspaltung $\mathfrak{L} \prec \mathfrak{Q}$ an Λ realisierbar ist; damit $\mathfrak{H}$ nicht mehr realisierbar ist, also zu $\mathfrak{Q}$ eine maximale Knotung von Λ gehört, müssen r und s Nichtreste für t sein. Die Behauptung folgt daraus, daß in $\mathfrak{Q}$ mod T immer noch $(R, S) \neq 1$ bleibt und mod RS noch $(R, T) = (S, T) \neq 1$, also $\mathsf{K}_0(\sqrt{r}, \sqrt{s})$ und $\mathsf{K}_0(\sqrt{rs}, \sqrt{t})$ knotbar sind, nicht aber etwa $\mathsf{K}_0(\sqrt{s}, \sqrt{t})$.

Schließlich bleibt für $\mathfrak{Z}$ die Bedingung, daß rs Rest für t, tr Rest für s und st Rest für r ist, ferner höchstens eins der r, s, t negativ; für „nur-$\mathfrak{Z}$“, daß außerdem kein Paar der r, s, t gegenseitig Rest ist. Die hemmende Bedingung folgt daraus, daß in $\mathfrak{Z}$ mod T schon $(R, S) = (R, T) = 1$ wird, also $\mathsf{P\Sigma}$ nicht knotbar ist, und daß umgekehrt hiermit (R, S) von (R, T) und (S, T) abhängig wird, unter der hemmenden Bedingung also jeder Kommutator von den beiden andern, was für $c = 2$ nicht mehr zutrifft. Wären ferner, was oben für $c > 1$ schon durch die anderen Angaben ausgeschlossen ist, zugleich r und s negativ, so wäre RS oder RST Trägheitselement einer unendlichen Primstelle, trotz seiner Ordnung 4 in $\mathfrak{Z}$. Daß endlich rs quadratischer Rest für t, also für alle seine Primteiler ist, ist sicher notwendig: wäre rs Nichtrest für den Teiler p von t, also etwa r Rest und s Nichtrest, so zerfiele p noch in P, aber nicht mehr in $\mathsf{P}(\sqrt{s})/\mathsf{P}$, und dann wäre $\Lambda/\mathsf{P} = \mathsf{P}(\sqrt{s}, \sqrt{t})$ knotenfrei, obwohl Z/P eine Knotung von Λ/P ist. Daß die drei quadratischen Restbedingungen auch hinreichen, folgt jedoch noch nicht aus [13]), sondern erst aus dem Richterschen Einbettungssatz in seiner zahlentheoretischen Fassung[14]): Der Zerlegungskörper eines t_i enthält sicher $\mathsf{K}_0(\sqrt{rs})$; seine Zerlegungsgruppe liegt also in $\{RS, T\}$; da in $\mathfrak{Z}$ nun $(RS, T) = 1$, stört t die Bildung eines Körpers $\mathfrak{Z}$ nicht.

Der Satz 4 aus [15]) sagt hier lediglich folgendes: Ist P in Λ für keinen Primteiler von

---

[11]) Vgl. auch H. Reichardt, Über Normalkörper mit Quaternionengruppe, Math. Zeitschr. **41** (1936), 218—221 und [10]) § 2, 3.

[12]) L. Rédei, Über die Klassenzahl des quadratischen Zahlkörpers, Math. Nat. Anz. d. Ung. Akad. 1931, 681, 707.

[13]) A. Scholz, Über die Lösbarkeit der Gleichung $t^2 - Du^2 = -4$, Math. Zeitschr. **39** (1925), 95—111, insbes. 97.

[14]) Vgl. [4]), 163 und Punkt 6.

[15]) A. Scholz, Die Kreisklassenkörper vom Primzahlpotenzgrad und die Konstruktion von Körpern mit vorgegebener zweistufiger Gruppe. II., Math. Ann. **110** (1935), 645.

st Zerlegungskörper, was oben immer erfüllt war, so ist Λ/P zu einem Diederkörper Λ' über P erweiterbar. Dieser braucht aber bei keiner Durchkreuzung ein absoluter Galoiskörper zu werden und wird es z. B. bei $\mathsf{P} = \mathsf{K}_0(\sqrt{-3})$ auch sicher nicht, wenn etwa Σ als Zerlegungskörper eines Primteilers von *rt* auftritt; sondern es kann dann Λ'/Λ den Führer $2 + \sqrt{-3}$ haben, der in P selbst wegen der Einheit -1 nicht als Führer auftritt. Daß dies jedoch, wenn Σ und T auch keine Zerlegungskörper in Λ sind, nicht eintritt, sondern der Führer ± 1 gewählt werden kann, entnehmen wir erst aus dem Richterschen Satz. Schon darum haben wir bei dem uns oben hauptsächlich interessierenden Fall $a = 0$, in dem K zwar einen Knoten, aber keine unmittelbare Knotung besitzt, Beispiele mit $c = 2, 3$ aufgesucht.

Ausführung der Durchkreuzung für das erste Beispiel:

Explizit sieht für $a > 0$ eine Konstruktion angegebener Art so aus; das wollen wir am ersten Tafelbeispiel $a = 4, c = 3$ zeigen, doch als Grundkörper dabei den Körper I der vierten Einheitswurzeln wählen, um zyklische Körper vierten Grades und Durchkreuzungen mit diesen durch vierte Wurzeln und Multiplikationen mit diesen bilden zu können: Sei

$$\mathsf{P} = \mathsf{I}(\sqrt{5}),\ \Sigma = \mathsf{I}(\sqrt{29}),\ \mathsf{T} = \mathsf{I}(\sqrt{109}),\ \Lambda = \mathsf{P}\Sigma\mathsf{T} \text{ und } \mathsf{K} = \mathsf{I}(\sqrt{145}, \sqrt{545}).$$

Bei $a = 4$ existieren alle drei Typen Diedererweiterungen $\Delta_r, \Delta_s, \Delta_t$ von K, in denen sich r, s, t weiterverzweigen, und der Typus Quaternionenerweiterung Θ von K mit Verzweigung von *rst*. Jeder dieser Körper Δ, Θ liegt in einer Durchkreuzung eines Körpers Z der oben definierten Gruppe $\mathfrak{Z}$ und Z bei $c = 3$ in einem Körper H einer Darstellungsgruppe $\mathfrak{H}$ von $\mathfrak{L}$ (s. o.), wo wieder $\mathsf{H} = \Phi\mathsf{X}\Psi$ das Produkt dreier Diedererweiterungen von $\mathsf{P}\Sigma, \mathsf{P}\mathsf{T}, \Sigma\mathsf{T}$ wird. Dabei sind Φ, X, Ψ erzeugbar durch

$$\varphi = \sqrt{2\sqrt{5} + \sqrt{29}},\quad \chi = \sqrt{5\sqrt{5} + \sqrt{109}},\quad \psi = \sqrt{5\sqrt{29} - 2\sqrt{109}}$$

(vierte Wurzeln aus Zahlen der Körper $\mathsf{I}(\sqrt{145})$, $\mathsf{I}(\sqrt{545})$ und $\mathsf{I}(\sqrt{29 \cdot 109})$, die so beschaffen sind, daß ihre Teilnormen in P und Σ, P und T, Σ und T Quadrate werden und damit Φ, X, Ψ normal über I). Setzt man $\varphi\chi\psi = \zeta$, so wird

$$\mathsf{Z} = \Lambda(\zeta) = \Lambda\left(\sqrt{289\sqrt{5} + 32\sqrt{29} + 45\sqrt{109}}\right) = \mathsf{I}(\zeta)$$

bei $\Lambda < \mathsf{I}(\zeta)$. Die Produkte $\zeta\sqrt[4]{5} = \delta_r$, $\zeta\sqrt[4]{29} = \delta_s$, $\zeta\sqrt[4]{109} = \delta_t$ und $\zeta\sqrt[4]{5 \cdot 29 \cdot 109} = \vartheta$ erzeugen jetzt bei

$$\delta_r = \sqrt{1445 + 32\sqrt{145} + 45\sqrt{545}},\ \ldots,\ \vartheta = \sqrt{1445\sqrt{3161} + 928\sqrt{545} + 4905\sqrt{145}}$$

bereits gewünschte Erweiterungen $\Delta_{r,s,t} = \mathsf{I}(\delta_{r,s,t})$ und $\Theta = \mathsf{I}(\vartheta)$. Denn Durchkreuzungen von Z über Λ mit den gewünschten Verzweigungen liefern nach der Galoistheorie der Kummerkörper (vgl. Hasse, Zahlbericht II, § 9 III. und § 10, (1)/(7)!) vorerst die Körper $\Lambda(\delta)$ und $\Lambda(\vartheta)$. In diesen sind aber die über K nur quadratischen $\mathsf{I}(\delta)$ und $\mathsf{I}(\vartheta)$ echt enthalten, und es zerfällt $\Lambda(\delta) = \Lambda\Delta$ und $\Lambda(\vartheta) = \Lambda\Theta$ direkt über K, wie gefordert.

Bemerkung: Sollen Φ, X, Ψ absolute Klk. über $\mathsf{P}\Sigma, \mathsf{P}\mathsf{T}, \Sigma\mathsf{T}$ werden und damit auch Z/Λ, so müssen $\varphi^2, \chi^2, \psi^2$ nicht nur wie hier Idealquadrate in den biquadratischen Körpern sein, sondern auch quadratische Reste mod 4 (multipliziert mit einer Potenz von $2i$), was sie durch Multiplikation mit $5 + 2i, 2 + i, 5 + 2i$ werden, also auch ζ^2 durch Multiplikation von ζ mit $\sqrt{2 + i}$.

Zugleich sind die Zusatzfaktoren so gewählt, daß dadurch die Substitutionen R, S, T von $\mathsf{P}, \Sigma, \mathsf{T}$ mit der ins Konjugiert-Komplexe überführenden Substitution J vertauschbar werden und damit I von allen Körpern $\Phi, \ldots, \mathsf{Z}$ direkt abspaltbar wird, insbesondere $\Phi, \ldots, \mathsf{Z}$ über dem rationalen Körper normal. (Es mußte z. B. für φ der Zusatzfaktor $\sqrt{5 + 2i}$ und nicht $\sqrt{1 + 2i}$ heißen, weil mit $\sqrt{29}^S = -\sqrt{29}$ die Teilnorm $(2\sqrt{5} + \sqrt{29})^{1+S} = -9$ und dann $\sqrt{2\sqrt{5} + \sqrt{29}}^{SJ-JS} = -1$ wird, wie auch $\sqrt{5 + 2i}^{SJ-JS} = -1$ bei $\sqrt{5 + 2i}^{1+J} = \sqrt{29}$.)

Um dasselbe Galoisverhalten für die Δ und Θ zu erreichen, müssen die Durchkreuzungsfaktoren $\sqrt[4]{5}, \sqrt[4]{29}, \sqrt[4]{109}$ einen Zusatzfaktor $\sqrt{\pm 1 \pm 2i}$, $\sqrt{\pm 5 \pm 2i}$, $\sqrt{\pm 3 \pm 10i}$ erhalten und dann z. B. δ_r insgesamt $\sqrt{i}$ und ϑ schließlich $\sqrt{56 + 5i}$ oder $\sqrt{44 + 35i}$. In den so normierten Δ, Θ bleibt 2 sowie jede zu $5 \cdot 29 \cdot 109$ prime Zahl unverzweigt.

Die reellen Unterkörper der neuen $\Phi, \mathsf{X}, \Psi, \mathsf{Z}, \Delta_{r,s,t}$ und Θ, die durch Abspaltung von I entstehen und die entsprechende Konstruktion bei rationalem Grundkörper liefern, werden hier durch die Realteile der normierten $\varphi, \ldots, \vartheta$ erzeugt, z. B. der reelle Δ_r durch $\sqrt{\frac{1}{2}(1445 + 45\sqrt{545}) + 16\sqrt{145}}$.

Zur Erläuterung von Satz 5 nehmen wir als Beispiel die Einbettung eines $\Sigma T = K_0(\sqrt{5}, \sqrt{101})$ enthaltenden Diederkörpers K in einen Normalkörper 16-ten Grades Λ mit der Gruppe $\mathfrak{L}$:

$$\mathfrak{L}: \qquad S^2 = T^2 = (S, T)^4 = 1$$

(dabei S und T die Trägheitssubstitutionen von 5 und 101 und

$$(S, T)^2 = ((S, T), S) = ((S, T), T),$$

also $\mathfrak{L}$ die Faktorgruppe der Ordnung 16 des freien Produkts der Zweiergruppe mit sich). Ein solcher Körper existiert nach [15]), weil 5 und 101 gegenseitig biquadratische Reste, und zwar hat nach [12]) der Körper $\Gamma = K_0(\sqrt{505})$ eine durch 8 teilbare Klassenzahl (hier genau 8), und es kann $\Lambda = \tilde{\Gamma}$ gesetzt werden. Der Unterkörper achten Grades K hat dann einen Knoten der Ordnung 2, weil Λ/K den in K unverzweigten Führer -1 hat. Durchkreuzt man jetzt aber etwa $K = \bar{\Gamma}$ mit $\sqrt{13}$, so muß sich 13 in Λ weiterverzweigen. K hat dann keinen Knoten, sondern nur einen 13-Strahlknoten der Ordnung 2. Soll ferner Λ in ein M der Ordnung 32 mit $S^2 = T^2 = 1$ eingebettet werden, so muß es reell sein, also bestimmt nicht $= \tilde{\Gamma}$ oder eine Durchkreuzung von $\tilde{\Gamma}/\bar{\Gamma}$, d. h. kein $\Lambda > \Sigma T$ hat einen Knoten mehr, doch bei Einbettbarkeit in ein M einen Strahlknoten.

Ob Knoten und Strahlknoten in K isomorph sind, war durch Satz 2/5 so entschieden: Isomorphie besteht, wenn eine zentrale Erweiterung Λ maximaler Knotung so gewählt werden kann, daß $\Lambda/K(\Lambda^0)$ zu K verzweigungsfremd ist. Das kann nun einmal wie oben bei K daran scheitern, daß eine Trägheitssubstitution beim Übergang von $\mathfrak{K}$ zu $\mathfrak{L}$ ihre Ordnung vergrößert wie oben (S, T), welche Gruppe des Geschlechts von $\mathfrak{L}$ man auch auswählt. Oder aber es liegt der Fall der D. M. V.-Aufgabe 194 vor, daß es bei festem $\mathfrak{K}$ und festen Trägheitsgruppen $\mathfrak{T}$ in $\mathfrak{K}$ zwar ein $\mathfrak{L}$ gibt, wo jedes $\mathfrak{T}$ eine zum Multiplikator fremde Vertretergruppe hat (was dann für die $\mathfrak{T} < \mathfrak{K}'$ im ganzen Geschlecht von $\mathfrak{L}$ gilt), aber keine zugehörige Erweiterung Λ von K.

Wir studieren diesen Fall so, daß wir $\Lambda/K\Lambda^0$ in Teilerweiterungen von Primzahlgrad zerlegen und vermerken, wo er eintritt, betrachten aber nur einfach verzweigte Körper. Sei also einfach Λ/K eine Knotung unverzweigten Primzahlgrades l und $\{T\}$ eine Trägheitsgruppe von $\mathfrak{K}$, die in der Gruppe $\mathfrak{L}$ von Λ ihre Ordnung von e auf el vergrößere, nicht aber in der zu $\mathfrak{L}$ verwandten Knotung $\mathfrak{N}$, zu der aber kein Körper N gehöre. Das tritt, da $\mathfrak{N}$ eine Durchkreuzung von $\mathfrak{L}$ mit einer zyklischen Verlängerung $\mathfrak{A}$ von $\mathfrak{K}^0$ ist, genau dann ein, wenn für wenigstens ein bei T verzweigtes $\mathfrak{p}$ zwar die Gruppe R der teilerfremden Reste mod $\mathfrak{p}$ in K eine durch el teilbare Ordnung hat, aber noch nicht deren K_0-Untergruppe R_0, weil sonst eine zu $\mathfrak{A}$ gehörige zyklische Verlängerung A von K^0 existierte, mit der Λ durchkreuzt ein N zu $\mathfrak{N}$ ergäbe.

Die angegebene Gestalt von R ist nun für zweierlei kennzeichnend: daß $\mathfrak{p}$ höheren Grad und eine Zerlegungsgruppe $\mathfrak{Z} = \{Z, T\}$ mit der Ableitung $\{T^e\}$ hat[14]), und daß $\mathfrak{p}$ nicht mehr Satz 8 gehorcht. Das letzte folgt so: Ist $\mathfrak{f} = \mathfrak{p}\mathfrak{h}$ der Führer von Λ/K, so gehören unter den $\alpha \equiv 1(\mathfrak{h})$ genau die l-ten Potenzreste mod $\mathfrak{p}$ zur Idealgruppe L von Λ; deren Normen sind nun el-te Potenzreste mod $\mathfrak{p}$ in K_0, was aber in R_0 nicht mehr sagt als e-ter Potenzrest, eine Eigenschaft, die bereits alle K/K_0-Zahlnormen haben. Also wird hier die L-Norm in keiner Weise durch eine Kongruenzangabe mod $\mathfrak{p}$ in K_0 gekennzeichnet, sondern erst in K. Da R zyklisch, gilt der Schluß auch rückwärts. — Die Aussage über die Zerlegungsgruppe folgt so: Ist $R = \{\varrho\}$, Ord $R_0 = ef$ und Z Frobenius-Substitution von $\mathfrak{p}$, also $\varrho^Z \equiv \varrho^{ef+1} \bmod \mathfrak{p}$; ist ferner Γ der Trägheitskörper von $\mathfrak{p}$, dabei $\mathfrak{p}\mathfrak{g}$ der Führer von K/Γ und $\tau \equiv \varrho\ (\mathfrak{p}),\ \equiv 1\,(\mathfrak{g})$, so gehört τ in der Klassengruppe von K/Γ zu T

(bei passender Wahl der Primitivwurzel ϱ), und es wird $\tau^{z-1} \equiv \tau^{el} \bmod \mathfrak{pg}$, also $T^{z-1} = (T, Z) = T^{el}$. Mithin $\mathfrak{Z}' = \{T^{el}\}$ und genau dann $= \{T^{e}\}$, wenn $(f, l) = 1$. Dies Doppelkriterium enthält dann Satz 10, wenn wir zuvor definieren:

$\mathfrak{v}$-*Grundstrahlnorm* heiße für invariantes verzweigtes, aber quadratfreies $\mathfrak{v}$ eine Norm, die $\equiv 1 \bmod \mathfrak{v}$ ist.

$\mathfrak{v}$-*Grundstrahlknoten* heiße die Faktorgruppe der totalen $\mathfrak{v}$-Strahlnormenreste nach den $\mathfrak{v}$-Grundstrahlnormen. Ohne Zusatz „$\mathfrak{v}$" ist wieder der Maximaltypus gemeint.

Doppelknoten heiße die Faktorgruppe der Grundstrahlnormen nach den Strahlnormen.

Bemerkung. Für die totalen Normenreste entsteht keine neue Definition, da sie ja stets durch Kongruenzen in K_0 mit Zusatz „Idealnorm" kennzeichenbar sind, und zwar auch mod $\mathfrak{v}$, wenn $\mathfrak{v}$ quadratfrei; während sonst auch oben „$\equiv 1 \bmod \mathfrak{v}$" in K_0 eine zu schwache Definition wäre. Natürlich sagt $N(\alpha) \equiv 1 \bmod \mathfrak{v}$ dasselbe wie $\equiv 1 \bmod \mathfrak{v}_0$, wo $\mathfrak{v}_0$ das niedrigste durch $\mathfrak{v}$ teilbare Ideal in K_0 ist.

Satz 10. *Der zu den Grundstrahlnormen mod* $\mathfrak{v}$ *gehörige Klassenkörper ist der maximale zentrale Klk.* M *mod* $\mathfrak{v}$ *über* K, *für den alle Zerlegungsgruppen in* M *Abelschen Aufspaltungen der entsprechenden Zerlegungsgruppen in* K *isomorph sind, m. a. W.: der* $\mathfrak{p}$*-adisch abgeschlossene* $\mathsf{M}_\mathfrak{p}$ *ist für alle* $\mathfrak{p}$ *noch eine Abelsche Erweiterung von* $\mathsf{K}_\mathfrak{p}$ *und maximal in seiner Art. Zum Doppelknoten gehören also die Teile zentraler Erweiterungen, die auch* $\mathfrak{p}$*-adisch für wenigstens ein* $\mathfrak{p}$ *nicht-Abelsch sind.*

Am Gesamtbild der Untersuchung ist folgendes typisch: Kennt man die Abelschen Körper über einem K_0, und betrachtet man Erweiterungen eines K/K_0 nicht als wesentlich verschieden, die durch Abelsche Durchkreuzung ineinander übergehen, was nur bei zentralen Erweiterungen vorkommt, so sind deren Idealgruppen im wesentlichen durch Zahlgruppen (Knoten!) gekennzeichnet, wie bei den $\mathfrak{p}$-adischen Klassenkörpern.

Zur Kennzeichnung der Galoisgruppe durch ihre Trägheitssubstitutionen als Erzeugende im Fall des rationalen Grundkörpers: Nach dem zahlentheoretischen Monodromiesatz[16]) wird die Galoisgruppe $\mathfrak{G}$ eines Normalkörpers Γ aus seinen Trägheitsgruppen erzeugt, und diese sind bei einfacher Verzweigung zyklisch. Sind $p, q, \ldots, t, \ldots$ die in Γ verzweigten Primzahlen und $P, Q, \ldots, T, \ldots$ erzeugende Trägheitssubstitutionen je eines ihrer Primteiler $\mathfrak{p}, \mathfrak{q}, \ldots, \mathfrak{t}, \ldots$ in Γ, so erzeugen diese mit ihren Konjugierten also $\mathfrak{G}$. Das von uns oben angewandte Verfahren, beim Übergang zu einem Oberkörper X wieder T als Trägheitserzeugende eines Primteilers von t zu verwenden durch Ersetzung von T durch einen Vertreter seiner Restklasse in der Galoisgruppe $\mathfrak{H} = \mathfrak{G} \cup \mathfrak{M}$ von X, wobei die Wahl zwischen diesem und seinen in $\mathfrak{M}$ Konjugierten bleibt, ist einheitlich so durchführbar: Man bilde eine Körperfolge $\mathsf{K}_1 < \mathsf{K}_2 < \cdots < \mathsf{K}_n < \cdots$, in der schließlich jedes einfach verzweigte Λ enthalten ist, und lasse bei einem in K_{n-1} bereits verzweigten t die Zuordnung $T \to \mathfrak{t}_{n-1}$ in K_n auf einen Primteiler $\mathfrak{t}_n$ von $\mathfrak{t}_{n-1}$ übergehen, während man bei einem in K_n neu verzweigten t einen beliebigen Primteiler $\mathfrak{t}_n$ von t durch T auszeichne. Auf diese Weise wird die Galoisgruppe eine Faktorgruppe der freien Gruppe $\{T_2, T_3, \ldots, T_p, \ldots\}$ mit $T_p = P$, in der u. a. für jedes T_p eine Relation $T_p^{p-1} = \Pi(Q, R)$ gilt, weil T_p in einem Kreiskörper höchstens die Ordnung $p - 1$ hat.

Für die in F. gegen Ende erwähnte Tschebotarëwsche Aufspaltung $\mathfrak{H} = \mathfrak{G}_T$ von $\mathfrak{G}$, in der die eingliedrigen Relationen $P^a = Q^b = \cdots = T^e = \cdots = 1$ von $\mathfrak{G}$ bestehen bleiben, die mehrgliedrigen $F(P, \ldots, T, \ldots) = 1$ aber durch $(F, \mathfrak{H}) = 1$ zu ersetzen sind, gilt nun

[16]) N. Tschebotarëw, Izvestija Kazan 1924.

Satz 11. *Bei rationalem Grundkörper hat der zentrale Klk. $\tilde{\Gamma}^*$ des Körpers Γ mit der Gruppe $\mathfrak{G}$ eine zur Tschebotarëwschen Aufspaltung $\mathfrak{G}_T$ homomorphe Gruppe. Isomorph ist sie sicher, wenn alle verzweigten Primideale den Grad 1 haben. Der Knoten von Γ ist dabei homomorph (isomorph) zum Ableitungsanteil des Multiplikators der Tschebotarëwschen Aufspaltung, also zum Multiplikator selbst, wenn die Trägheitserzeugenden von Γ^0 für $\mathfrak{G}^0$ eine Basis bilden.*

Die Homomorphieaussagen folgen dabei aus Satz 2, weil bei rationalem Grundkörper Λ so durchkreuzt werden kann, daß Λ/Γ als Führer ± 1 hat[4]). Die Isomorphien folgen dann aus dem speziellen Einbettungssatz in [4]).

Zur Untersuchung der zentralen Erweiterungen wird es meist genügen, wie bei den Beispielen auf S. 229, die zweigliedrigen Relationen der Art $S^a T = 1$ bestehen zu lassen und so in $\tilde{\Gamma}^*$ direkte Teile von $\tilde{\Gamma}^0$ fortzulassen.

Weitere Ausführungen mit besonderer Berücksichtigung der Tschebotarëwschen Begriffsbildungen seien einer Abhandlung über die zentralen Verzweigungen vorbehalten.

Eingegangen 2. September 1939.

Über separable, abgeschlossene Abelsche Gruppen[1]).

Von *Wolfgang Krull* in Bonn.

Gegenstand der folgenden Betrachtung ist das Problem der direkten Summenzerlegung additiv geschriebener, abgeschlossener Abelscher Gruppen in „*einrangige*“ oder „*zyklische*“ Summanden[2]). Unsern Ausgangspunkt bilden die bahnbrechenden Arbeiten von H. Prüfer[3]). Prüfer zeigte bekanntlich als erster, daß eine unendliche Abelsche Gruppe — anders als im endlichen Fall — i. a. nicht zyklisch zerlegbar ist, auch dann nicht, wenn man sich auf Gruppen beschränkt, die nur Elemente endlicher Ordnung enthalten. Auf der andern Seite gelang es Prüfer, wenigstens bei den abzählbaren Gruppen des zuletzt genannten Typs notwendige und hinreichende Bedingungen für die Möglichkeit der zyklischen direkten Zerlegung aufzustellen. An diese ersten Prüferschen Ergebnisse, die für eine im gewissen Sinne abschließende Arbeit von H. Ulm[4]) grundlegend geworden sind, werden wir im folgenden nicht anknüpfen. Von entscheidender Wichtigkeit dagegen für uns sind weitergehende Untersuchungen Prüfers, bei denen er den Begriff der „*idealen*“ oder „*abgeschlossenen*“ (Abelschen) Gruppen einführte[5]).

Eine abgeschlossene Gruppe ist dadurch gekennzeichnet, daß sie hinsichtlich eines ausgezeichneten, durch gewisse Untergruppen und ihre Nebenscharen (Nebengruppen) definierten Umgebungssystems einen „abgeschlossenen“[5a]) topologischen Raum bildet. Prüfer zeigte, daß jede abgeschlossene Gruppe endlichen Ranges zyklisch direkt zerlegbar ist; im allgemeinsten abgeschlossenen Fall erklärte er sich für außerstande, eine Entscheidung zu treffen. Pietrkowski dagegen glaubte, die Möglichkeit der zyklischen direkten Zerlegung beliebiger abgeschlossener Gruppen beweisen zu können, doch zeigte später Pontrjeagin durch ein Gegenbeispiel, daß es tatsächlich zyklisch direkt unzerlegbare, abge-

[1]) Der erste Teil der Note gibt im wesentlichen den Inhalt meines im Sommer 1939 in Göttingen gehaltenen Vortrags wieder. Der zweite Teil mit seinen positiven Ergebnissen geht über den damals erreichten Standpunkt wesentlich hinaus.

[2]) Der allgemeine Begriff der einrangigen oder zyklischen Gruppe geht auf Prüfer zurück (vgl. [3])). Die für uns wichtigen Typen einrangiger Gruppen werden weiter unten im Text genau beschrieben. — Die direkte Summe $\mathfrak{A}_1 + \mathfrak{A}_2 + \cdots + \mathfrak{A}_n$ endlich vieler Gruppen $\mathfrak{A}_i$ wird wie üblich definiert. Zur Definition der direkten Summe unendlich vieler Gruppen vgl. man die Betrachtungen weiter unten im Text.

[3]) H. Prüfer, [1] Untersuchungen über die Zerlegbarkeit der abzählbaren primären Abelschen Gruppen, Math. Zeitschrift **17** (1923), 35—61. — [2] Theorie der Abelschen Gruppen I., Math. Zeitschrift **20** (1924), 165—187. — [3] Theorie der Abelschen Gruppen II. Ideale Gruppen, Math. Zeitschrift **22** (1925), 222—249.

[4]) H. Ulm, Theorie der abzählbar-unendlichen Abelschen Gruppen, Math. Annalen **107** (1932), 774—803.

[5]) „Ideale“ Gruppen im Sinne von Prüfer[3]) [3]. Wir sprechen im folgenden durchweg von „abgeschlossenen“ Gruppen, da diese Bezeichnungsweise der für uns maßgebenden topologischen Auffassung besser entspricht.

[5a]) Die „Abgeschlossenheit“ besteht darin, daß jede Cauchy-konvergente Folge in der als Raum aufgefaßten Gruppe einen Grenzwert besitzt. Im übrigen vgl. zu den topologischen Eigenschaften der separablen Gruppen den „Zusatz bei der Korrektur“ am Schluß der Note.

schlossene Gruppen gibt[6]). Im folgenden soll zuerst der in den Pietrkowskischen Schlüssen steckende Fehler aufgedeckt werden. Später wenden wir uns dann der Aufstellung von notwendigen und hinreichenden Bedingungen für die zyklische direkte Zerlegbarkeit „separabler" abgeschlossener Gruppen zu.

Der Einfachheit halber beschränken wir uns von vornherein auf „*primäre*" Abelsche Gruppen, was nach Prüfer und Pietrkowski keine wesentliche Beeinträchtigung der Allgemeinheit bedeutet. Die Gruppe A heißt *primär* (und zwar zur Primzahl p gehörig), wenn sie gleichzeitig mit α stets auch $n \cdot \alpha$ enthält, wobei n eine beliebige ganze p-adische Zahl bedeutet[7]). Eine ausschließlich aus Elementen endlicher Ordnung bestehende Gruppe ist dann und nur dann primär, wenn bei jedem Element die Ordnung eine Potenz von p darstellt. In einer beliebigen primären Gruppe A ist für jedes α und jedes ganze, zu p teilerfremde p-adische r die Gleichung $r \cdot \xi = \alpha$ eindeutig lösbar; was die Primzahl p angeht, so wird *in* A dem Element α die *Höhe* p^n zugeschrieben, wenn zwar die Gleichung $p^n \cdot \xi = \alpha$, nicht aber die Gleichung $p^{n+1} \cdot \xi = \alpha$ in A (mindestens) eine Lösung besitzt. Gibt es für jedes n in A ein α_n mit $p^n \cdot \alpha_n = \alpha$, so ist die Höhe von α in A gleich ∞ („unendlich") zu setzen. Eine primäre Gruppe heißt „*einrangig* oder *zyklisch*", wenn sie isomorph ist entweder a) zur Additionsgruppe $\mathfrak{R}$ aller ganzen p-adischen Zahlen, oder b) zur Additionsgruppe $\mathfrak{K}$ aller rationalen p-adischen Zahlen, oder c) zu einer Restklassengruppe $\mathfrak{R}/p^n \cdot \mathfrak{R}$, oder d) zur Restklassengruppe $\mathfrak{K}/\mathfrak{R}$. Die Gruppen vom Typus a), b) enthalten (außer 0) keine Elemente endlicher Ordnung; die vom Typus c) sind die gewöhnlichen endlichen Abelschen Gruppen. Eine Gruppe vom Typus d) enthält nur Elemente endlicher Ordnung und unendlicher Höhe; sie besitzt ein Erzeugendensystem $\alpha_1, \alpha_2, \alpha_3, \ldots$ mit den Relationen $p \cdot \alpha_1 = 0$, $p \cdot \alpha_{i+1} = \alpha_i$ $(i = 1, 2, \ldots)$.

Bei den abgeschlossenen primären Gruppen, deren alleiniger Betrachtung wir uns nunmehr endgültig zuwenden, untersuchen wir — und das bedeutet natürlich eine wesentliche Einschränkung der Allgemeinheit — ausschließlich *separable* Gruppen, bei deren Topologisierung man mit einem abzählbaren Umgebungssystem auskommt. Eine abgeschlossene separable Gruppe $\mathsf{A} = \mathsf{A}_0$ ist charakterisiert durch die Existenz einer Untergruppenkette $\mathsf{A}_0 > \mathsf{A}_1 > \mathsf{A}_2 > \cdots$ mit den folgenden drei Eigenschaften:

1. *Der Durchschnitt aller* A_i *ist gleich dem Nullideal,* $\Delta \mathsf{A}_i = (0)$.

2. *Die Restklassengruppen* $\mathsf{A}_i/\mathsf{A}_{i-1}$ $(i = 1, 2, \ldots)$ *sind sämtlich zyklisch von den Typen* c) *oder* d).

3. *Ein unendliches Kongruenzensystem* $\xi \equiv \alpha_i(\mathsf{A}_i)$, *das der „Verträglichkeitsbedingung"* $\alpha_{i+1} \equiv \alpha_i(\mathsf{A}_i)$ $(i = 1, 2, \ldots)$ *genügt, besitzt in* A *stets eine* (*wegen* 1. *eindeutig bestimmte*) *Lösung*[8]).

---

[6]) St. Pietrkowski, Theorie der unendlichen Abelschen Gruppen, Math. Annalen **104** (1931), 535—569. — L. Pontrjeagin, The theory of topological commutative groups, Annals of Math. Princeton (2) **35** (1934), 361—388.

[7]) Genauer ausgedrückt: Es muß für beliebiges ganzes p-adisches n und für beliebiges α aus A das Produkt $n \cdot \alpha$ stets definiert und gleich einem eindeutig bestimmten Elemente β aus A sein, wobei insbesondere stets

$$2 \cdot \alpha = \alpha + \alpha,\ 3 \cdot \alpha = \alpha + \alpha + \alpha, \ldots$$

wird. — Zur Tatsache, daß jede abgeschlossene primäre Abelsche Gruppe eindeutig als direkte Summe i. a. unendlich vieler, zu verschiedenen Primzahlen gehöriger, primärer abgeschlossener Gruppen darstellbar ist, vgl. Pietrkowski [6]) § 4; ein entsprechender Satz über eine direkte Durchschnittsdarstellung beliebiger abgeschlossener Abelscher Gruppen findet sich bereits bei Prüfer [3]) [3], § 7.

[8]) Man überzeugt sich leicht, daß jede mit Hilfe eines abzählbaren Umgebungssystems topologisierbare primäre abgeschlossene Gruppe die Eigenschaften 1., 2., 3. besitzt und umgekehrt. — Es ist daher zulässig (und hier der Kürze halber empfehlenswert) die separablen primären Gruppen geradezu durch die Eigenschaften 1., 2., 3. zu definieren. — Als separabel sind auch die endlichen Abelschen Gruppen anzusehen, sowie allgemeiner alle die Gruppen, die sich als direkte Summe von endlich vielen zyklischen Summanden des Typus c) oder d) darstellen lassen; es sind das diejenigen Gruppen, bei denen die Kette $\mathsf{A}_0, \mathsf{A}_1, \mathsf{A}_2, \ldots$ nach endlich vielen Schritten mit der Nullgruppe abbricht.

Setzen wir den „*Betrag*“ $|\alpha|$ eines Elementes α, das zu A_i, aber nicht zu A_{i+1} gehört, gleich e^{-i} ($|0| = 0$!), so können wir der Bedingung 3, der eigentlichen „Abgeschlossenheitsbedingung“ auch die folgende Fassung geben:

3*. *Eine formale unendliche Summe* $\alpha_1 + \alpha_2 + \alpha_3 + \cdots$, *die der Konvergenzbedingung* $\lim\limits_{i\to\infty} |\alpha_i| = 0$ *genügt, besitzt in* A *stets einen durch die Gleichung*

$$\lim_{i\to\infty} |\alpha - (\alpha_1 + \cdots + \alpha_i)| = 0$$

eindeutig gekennzeichneten Grenzwert α.

Im folgenden bedeutet, sofern nichts anderes ausdrücklich bemerkt wird, „Gruppe“ immer soviel wie „abgeschlossene Gruppe“. Prüfer hat gezeigt, daß von jeder selbst nicht zyklischen Gruppe A ein zyklischer direkter Summand Z abgespalten werden kann, $\mathsf{A} = \mathsf{Z} + \mathsf{B}$[9]. Daraus würde sich nach Pietrkowski sehr leicht die zyklische direkte Zerlegbarkeit beliebiger Gruppen ergeben, wenn ein gewisser, auf transfinite Induktion zugeschnittener *Konstruktionssatz* richtig wäre, der im Falle des ersten Limesschrittes folgendermaßen lautet:

Es seien zu gegebenem $\mathsf{A} = \mathsf{B}_0$ die Untergruppen $\mathsf{Z}_1, \mathsf{Z}_2, \ldots; \mathsf{B}_1, \mathsf{B}_2, \ldots$ so bestimmt, daß alle Z_i zyklisch sind, und daß durchweg $\mathsf{B}_{i-1} = \mathsf{Z}_i + \mathsf{B}_i$ wird ($i = 1, 2, \ldots$). Bedeutet dann Γ die (abgeschlossene!) kleinste gemeinsame Obergruppe aller Z_i, Δ den Durchschnitt aller B_i, so wird stets $\mathsf{A} = \Gamma + \Delta$.

Leider ist der Konstruktionssatz falsch. Es soll unsere nächste Aufgabe sein, unter Beschränkung auf den ersten Limesschritt den dem Pietrkowskischen Scheinbeweis zugrunde liegenden, an sich bemerkenswerten Trugschluß genauer zu analysieren.

Da jede der Gruppen Z_i zur (abgeschlossenen) kleinsten gemeinsamen Obergruppe aller Z_k ($k \neq i$) elementefremd ist, liegt es nahe, Γ als die direkte unendliche Summe der Gruppen $\mathsf{Z}_1, \mathsf{Z}_2, \ldots$ anzusehen, $\Gamma = \mathsf{Z}_1 + \mathsf{Z}_2 + \cdots$. Auf der andern Seite aber überzeugt man sich leicht, *daß es nur dann einen Sinn hat, von der „direkten Summe* $\Gamma = \mathsf{Z}_1 + \mathsf{Z}_2 + \cdots$“ *zu reden, wenn* Γ *aus allen und nur den unendlichen Elementsummen* $\zeta_1 + \zeta_2 + \cdots$ (ζ_i *beliebig aus* Z_i) *besteht*[10]).

In der Tat nimmt Pietrkowski stillschweigend an, daß Γ immer diese einfache Gestalt besitzt. Aber gerade diese Voraussetzung ist der entscheidende Fehler. Man sieht nämlich leicht:

Γ *besteht dann und nur dann aus allen Summen* $\zeta_1 + \zeta_2 + \cdots$, *es darf also dann und nur dann* $\Gamma = \mathsf{Z}_1 + \mathsf{Z}_2 + \cdots$ *geschrieben werden, wenn* $\lim\limits_{i\to\infty} |\mathsf{Z}_i| = 0$ *ist für*

$$|\mathsf{Z}_i| = \max |\zeta_i| \quad (\zeta_i < \mathsf{Z}_i).$$

Daß aber die Konvergenzbedingung $\lim\limits_{i\to\infty} |\mathsf{Z}_i| = 0$ keineswegs immer erfüllt ist, kann durch ganz einfache Beispiele belegt werden, und damit ist dem Pietrkowskischen Beweis der Boden entzogen[11]).

---

[9]) Vgl. Prüfer [3]) [3], § 14.

[10]) Würde man an dieser Forderung nicht festhalten, so würde z. B. der unbedingt notwendige Satz, daß eine unendliche direkte Summe (ebenso wie eine endliche) durch Angabe ihrer Summanden bis auf Isomorphie eindeutig bestimmt ist, nicht mehr allgemein gelten. — Natürlich dürfen bei einer unendlichen direkten Summe $\Gamma = \mathsf{Z}_1 + \mathsf{Z}_2 + \cdots$ zwei Elementsummen $\zeta_1 + \zeta_2 + \cdots$ und $\zeta_1' + \zeta_2' + \cdots$ nur dann gleich sein, wenn die entsprechenden Summanden paarweise gleich sind, $\zeta_i = \zeta_i'$ ($i = 1, 2, \ldots$).

[11]) Es sei $\mathsf{Z}_i = (\alpha_i)$ eine zyklische Gruppe der Ordnung p mit dem erzeugenden Element α_i, unter $\mathsf{A}_{i-1} = \mathsf{Z}_i + \mathsf{Z}_{i+1} + \cdots$ ($i = 1, 2, \ldots$) möge die unendliche direkte Summe der Gruppen $\mathsf{Z}_i, \mathsf{Z}_{i+1}, \ldots$ im Sinne des Textes verstanden werden. Die Beträge der Elemente seien in der abgeschlossenen Gruppe $\mathsf{A} = \mathsf{A}_0$ mit Hilfe der charakteristischen Untergruppenkette $\mathsf{A}_0, \mathsf{A}_1, \mathsf{A}_2, \ldots$ definiert. Ferner werde

$$\beta_i = \alpha_1 + \alpha_2 + \cdots + \alpha_i, \quad \mathsf{Z}_i' = (\beta_i), \quad \mathsf{B}_i = \mathsf{A}_{i+1} + \mathsf{Z}_{i+1}' \quad (i = 1, 2, \ldots)$$

Auf der andern Seite erkennt man mühelos, und damit kommen wir zum zweiten Teil unserer Betrachtungen: *Es sei eine Klasse K von separablen Gruppen gegeben, die der folgenden Bedingung genügt: Eine beliebige Gruppe* A *aus K mit der charakteristischen Untergruppenkette* $\mathsf{A}_1, \mathsf{A}_2, \ldots$ *besitzt stets eine direkte Summenzerlegung* $\mathsf{A} = \mathsf{Z}_1 + \cdots + \mathsf{Z}_n + \mathsf{B}$, *bei der die* Z_i *zyklisch sind, während die gleichfalls zu K gehörige Gruppe* B *in* A_1 *enthalten ist. — Dann ist jede Gruppe* A *aus K zyklisch direkt zerlegbar,* $\mathsf{A} = \mathsf{Z}_1 + \mathsf{Z}_2 + \mathsf{Z}_3 + \cdots$.

Mit Hilfe dieser Bemerkung zeigt man zunächst sehr leicht, *daß eine separable Gruppe* A *immer zyklisch direkt zerlegbar ist, wenn sie entweder* 1) *kein Element endlicher Ordnung enthält, oder wenn sie* 2) *ein Erzeugendensystem von Elementen endlicher Ordnung besitzt*[12]) *und dabei von Elementen unendlicher Höhe frei ist.*

Schwieriger dagegen ist es, bei beliebigen separablen Gruppen zu einfachen Aussagen zu kommen. Wir führen hier zuerst einige abkürzende Bezeichnungen ein:

Eine Gruppe ohne Elemente endlicher Ordnung möge *unverknotet* (torsionsfrei), eine Gruppe mit einem Erzeugendensystem von Elementen endlicher Ordnung möge *Knotengruppe* genannt werden. Unter der „*zu einer gegebenen Gruppe* A *gehörigen Knotengruppe* E“ *verstehen wir die größte in* A *enthaltene Knotengruppe*, also die kleinste Untergruppe von A, in der alle Elemente endlicher Ordnung aus A liegen[13]). — Führt man die gleichen Begriffsbildungen bei den gewöhnlichen Abelschen Gruppen ein, so erhält man sofort die Sätze: „Eine Gruppe ist dann und nur dann Knotengruppe, wenn sie ausschließlich aus Elementen endlicher Ordnung besteht. Jede Untergruppe einer Knotengruppe ist selbst Knotengruppe. Die Restklassengruppe A/E einer beliebigen Gruppe A nach der zugehörigen Knotengruppe E ist stets unverknotet.“ — Bei unseren abgeschlossenen Gruppen dagegen liegen die Dinge ganz anders.

Aus der Tatsache, daß eine konvergente Summe von Elementen endlicher Ordnung keineswegs selbst eine endliche Ordnung zu besitzen braucht, folgt sofort, *daß eine Knotengruppe im allgemeinen Elemente unendlicher Ordnung und damit auch* (*abgeschlossene*!) *unverknotete Untergruppen enthält.* Unter diesen Umständen muß aber A/E keineswegs immer unverknotet sein. Man kann sogar leicht separable Gruppen A konstruieren, bei denen jedes Element eine endliche Höhe hat, und bei denen gleichwohl in A/E Elemente endlicher Ordnung auftreten[14]).

---

gesetzt. Dann ist $\mathsf{A} = \mathsf{B}_0 = \mathsf{Z}_1' + \mathsf{B}_1$, $\mathsf{B}_{i-1} = \mathsf{Z}_i' + \mathsf{B}_i$ $(i = 1, 2, \ldots)$. Aber es kann die (wegen $\mathsf{Z}_1 + \cdots + \mathsf{Z}_i = \mathsf{Z}_1' + \cdots + \mathsf{Z}_i'$ mit A zusammenfallende) kleinste gemeinsame Obergruppe Γ aller Z_i' nicht als direkte Summe der Z_i' bezeichnet werden, weil wegen $|\beta_i| = |\mathsf{Z}_i'| = 1$ $(i = 1, 2, \ldots)$ die Konvergenzbedingung $\lim_{i\to\infty} |\mathsf{Z}_i'| = 0$ nicht erfüllt ist. (Man beachte z. B., daß einerseits in A die unendliche Summe $\beta_1 + \beta_2 + \beta_3 + \cdots$ keinen Sinn hat, und daß andrerseits das zu $\Gamma = \mathsf{A}$ gehörige Element $\alpha_1 + \alpha_2 + \alpha_3 + \cdots$ keine Darstellung

$$\alpha_1 + \alpha_2 + \alpha_3 + \cdots = n_1 \cdot \beta_1 + n_2 \cdot \beta_2 + n_3 \cdot \beta_3 + \cdots \quad (n_1, n_2, n_3, \ldots \text{ ganze } p\text{-adische Zahlen})$$

besitzt.) — Im übrigen sei noch bemerkt, daß in unserem Falle auch die Gleichung $\mathsf{A} = \Gamma + \Delta$ nicht gilt, falls Δ den Durchschnitt aller B_i bedeutet. Denn es ist ja, wie bereits hervorgehoben, $\mathsf{A} = \Gamma$, und es stellt Δ nicht die Nullgruppe dar, weil das von 0 verschiedene Element $\alpha_1 + \alpha_2 + \alpha_3 + \cdots$ zu allen B_i gehört.

[12]) Das endliche oder abzählbar unendliche Elementsystem $\alpha_1, \alpha_2, \ldots$ aus A heißt ein Erzeugendensystem von A, wenn jedes Element γ aus A in der Form $\gamma = n_1 \cdot \alpha_1 + n_2 \cdot \alpha_2 + \cdots$ $(n_1, n_2, \ldots$ ganze p-adische Zahlen$)$ dargestellt werden kann.

[13]) Unsere Bezeichnungsweise knüpft an die Tatsache an, daß gewöhnliche Abelsche Gruppen ohne Elemente endlicher Ordnung neuerdings (mit Rücksicht auf gewisse Beziehungen zur Topologie) „torsionsfrei“ genannt werden. — „Ohne Elemente endlicher Ordnung“ heißt natürlich soviel wie „ohne von 0 verschiedene Elemente endlicher Ordnung“.

[14]) Es sei $\mathsf{Z}_i = (\alpha_i)$ eine zyklische Gruppe der Ordnung p^i mit dem erzeugenden Element α_i, unter $\mathsf{A}_i = \mathsf{Z}_i + \mathsf{Z}_{i+1} + \cdots$ möge die unendliche direkte Summe der Gruppen $\mathsf{Z}_i, \mathsf{Z}_{i+1}, \ldots$ verstanden werden $(i = 1, 2, \ldots)$. A_1 ist eine separable Gruppe mit der charakteristischen Untergruppenkette $\mathsf{A}_1, \mathsf{A}_2, \ldots$ und zwar stellt A_1 eine Knotengruppe dar, weil die Elemente $\alpha_1, \alpha_2, \ldots$ ein Erzeugendensystem von A_1 bilden; dabei enthält A_1 auch Elemente unendlich hoher Ordnung, z. B. $\gamma = \alpha_1 + \alpha_2 + \cdots$. Wir bilden zu A_1 nun eine Obergruppe $\mathsf{A} = \mathsf{A}_1(\xi)$, indem wir ein

Auf der andern Seite ist bei einer zyklisch direkt zerlegbaren Gruppe A die Restklassengruppe $\mathsf{A/E}$ immer unverknotet.

Schreibt man nämlich eine bestimmte zyklische direkte Zerlegung von A in der Form $\mathsf{A} = (\mathsf{Z}_1 + \mathsf{Z}_2 + \cdots) + (\mathsf{Z}'_1 + \mathsf{Z}'_2 + \cdots) = \Phi + \Psi$, wobei im Sinne unserer früheren Einteilung alle Z_i zum Typus a) oder b), alle Z'_i zum Typus c) oder d) gehören, so wird offenbar $\Psi = \mathsf{E}$ und es erweist sich $\mathsf{A/E}$ als isomorph zu der sicher unverknoteten Gruppe Φ. Wir haben also den Satz:

Es gibt separable Gruppen, sogar solche ohne Elemente unendlicher Höhe, die nicht zyklisch direkt zerlegbar sind[15]). — Besonders wichtig ist dabei die Tatsache, daß wir nicht nur über ein einzelnes, „pathologisch" anmutendes Beispiel, sondern über eine systematische Methode zur Bildung recht einfacher Beispiele verfügen.

Weit bedeutsamer noch als dieses negative Ergebnis ist indessen die Erkenntnis, daß unsere Überlegungen uns zur Aufstellung von notwendigen und hinreichenden Bedingungen für die zyklische direkte Zerlegbarkeit beliebiger separabler Abelscher Gruppen führen. Zunächst zeigt man leicht:

Eine separable Gruppe A *ohne Elemente unendlicher Höhe ist dann und nur dann zyklisch direkt zerlegbar, wenn die Restklassengruppe* $\mathsf{A/E}$ *von* A *nach der zugehörigen Knotengruppe* E *unverknotet ist.*

Es sei nämlich $\mathsf{A} = \mathsf{A}_0, \mathsf{A}_1, \ldots$ eine charakteristische Untergruppenkette von A, und es bedeute $\bar{\alpha}$ eine erzeugende Restklasse der in unserm Falle sicher endlichen Gruppe $\mathsf{A/A}_1$. Wählt man dann in $\bar{\alpha}$ einen Repräsentanten α *von möglichst kleiner Ordnung*, so erweist sich die durch α erzeugte zyklische Gruppe $\mathsf{Z} = (\alpha)$ als eine „Servanzuntergruppe" von A im Sinne Prüfers, es gibt daher nach Prüfer[3]) [3] § 12 mindestens eine direkte Summenzerlegung $\mathsf{A} = \mathsf{Z} + \mathsf{B}$, und man kann dabei insbesondere, wie leicht zu sehen, B als Untergruppe von A_1 wählen. Da nun B gleichzeitig mit A zur Klasse K aller separablen Gruppen ohne Elemente unendlicher Höhe gehört, muß nach dem oben aufgestellten allgemeinen Lemma A zyklisch direkt zerlegbar sein.

Schwieriger gestaltet sich die Untersuchung, wenn wir uns beliebigen separablen Gruppen mit Elementen unendlicher Höhe zuwenden. Hier tritt zu der Bedingung der Unverknotetheit von $\mathsf{A/E}$ noch eine Zusatzforderung, zu der uns die folgende Überlegung führt: Es sei E eine Knotengruppe, Φ die aus allen Elementen unendlicher Höhe bestehende Untergruppe von E. Ist dann $\mathsf{E} = \mathsf{Z}_1 + \mathsf{Z}_2 + \cdots$ eine zyklische direkte Zerlegung von E, so wird Φ offenbar gleich der direkten Summe aller der Z_i, die im Sinne unserer früheren Klassifikation den Typus d) besitzen, und daraus ergibt sich sofort, daß Φ ebenso wie E selbst eine Knotengruppe sein muß. — Wir definieren nun angesichts dieser Feststellung: Die separable Gruppe A mit der zugehörigen Knotengruppe E soll „*korrekt verknotet*" heißen, wenn 1) $\mathsf{A/E}$ unverknotet ist, und wenn 2) die Untergruppe aller Elemente unendlicher Höhe aus E selbst eine Knotengruppe darstellt. Dann gilt der Hauptsatz:

Eine separable Gruppe A *ist dann und nur dann zyklisch direkt zerlegbar, wenn sie korrekt verknotet ist.*

Beim Beweise des Hauptsatzes, bei dem es nach den bisherigen Betrachtungen einzig noch auf das „dann" ankommt, erledigt man zunächst sehr leicht den Spezialfall einer beliebigen unverknoteten Gruppe A. (Jede derartige Gruppe ist ja im Sinne un-

---

Element ξ hinzunehmen, von dem wir festsetzen, daß $p \cdot \xi = \gamma$ werden soll. A ist dann eine separable Gruppe mit der charakteristischen Untergruppenkette $\mathsf{A}, \mathsf{A}_1, \mathsf{A}_2, \ldots$. Die zugehörige Knotengruppe ist $\mathsf{E} = \mathsf{A}_1$, wie sofort aus der Tatsache folgt, daß nicht nur γ selbst, sondern auch jedes Element der Form $\gamma + p \cdot \delta$ (δ in A_1) unendlich hohe Ordnung besitzt. $\mathsf{A/E} = \mathsf{A/A}_1$ aber ist nicht unverknotet, sondern zyklisch von der Ordnung p.

[15]) Vgl. hierzu auch Pontrjeagin [6]) S. 383, example 1. — Vgl. auch den „Zusatz bei der Korrektur" am Schlusse der Note.

serer Definition korrekt verknotet.) Der zweite Schritt besteht in dem bereits etwas mühsameren Nachweis, daß der Hauptsatz allgemein gilt, falls er nur für jede korrekt verknotete Knotengruppe richtig ist. Bei der Behandlung einer korrekt verknoteten Knotengruppe E schließlich tritt die eigentliche Schwierigkeit des Problems zutage, auf die wir hier wenigstens andeutungsweise eingehen wollen.

Es sei $\mathsf{E}, \mathsf{E}_1, \mathsf{E}_2, \ldots$ eine charakteristische Untergruppenkette von E, und es sei dabei, um gleich den kritischen Fall ins Auge zu fassen, $\bar{\mathsf{E}} = \mathsf{E}/\mathsf{E}_1$ eine zyklische Gruppe vom Typus d) mit einem Erzeugendensystem $\bar{\alpha}_1, \bar{\alpha}_2, \ldots$ mit den Relationen $p \cdot \bar{\alpha}_i = \bar{\alpha}_{i-1}$ $(i = 1, 2, \ldots; \bar{\alpha}_0 = \bar{0})$. Dann zeigt man zunächst (und das ist der entscheidende Schritt) unter wesentlicher Ausnutzung der Tatsache, daß E korrekt verknotet ist: Es läßt sich für hinreichend großes i in $\bar{\alpha}_i$ ein Repräsentant α_i so auswählen, daß einerseits α_i unendliche Höhe, aber endliche Ordnung besitzt, und daß andrerseits bei keinem einzigen Repräsentanten α_i' von $\bar{\alpha}_i$ die Ordnung kleiner wird als bei α_i. Auf Grund dieses Resultats beweist man weiter verhältnismäßig einfach die Existenz einer direkten Summenzerlegung $\mathsf{E} = \mathsf{Z} + \mathsf{Z}_1 + \cdots + \mathsf{Z}_k + \mathsf{E}'$ $(k < i)$, bei der die korrekt verknotete Knotengruppe E' ganz in E_1 enthalten ist, während Z eine zyklische Gruppe vom Typus d) darstellt und die Z_ν $(\nu = 1, \ldots, k)$ endliche zyklische Gruppen sind. Damit ist dann angesichts unseres früheren Lemmas im wesentlichen alles erledigt.

Kritisch ist zu dem für unsere Betrachtungen entscheidenden Begriff der „korrekten Verknotung" mit den Bedingungen 1) und 2) folgendes zu bemerken: Daß man leicht separable Gruppen angeben kann, die zwar der Bedingung 2), nicht aber der Bedingung 1) genügen, wurde bereits oben festgestellt. Dagegen ist es mir noch nicht gelungen, eine Gruppe zu konstruieren, bei der 1), aber nicht 2) erfüllt ist[15a]). Es besteht also immer noch die (von mir gefühlsmäßig bezweifelte) Möglichkeit, daß die sämtlichen korrekt verknoteten Gruppen A *allein* durch die Unverknotetheit von A/E charakterisiert werden können.

Indessen kam es uns hier im wesentlichen darauf an, überhaupt einmal notwendige und hinreichende Bedingungen für die zyklische direkte Zerlegbarkeit separabler Gruppen aufzustellen. Dieses Ziel haben wir erreicht, und dabei die wichtige Erkenntnis gewonnen: Die in der Theorie der separablen Gruppen auftretenden Schwierigkeiten entspringen alle aus dem einen Umstand, daß eine Folge von Elementen endlicher Ordnung gegen einen Grenzwert unendlich hoher Ordnung konvergieren kann. *Man hat es also mit Schwierigkeiten „analytischen" Charakters zu tun, die in der Theorie der gewöhnlichen abzählbaren Abelschen Gruppen kein Gegenstück besitzen.*

Für die Anwendung unserer Ergebnisse im Einzelfalle kommt vor allem die Galoissche Theorie in Betracht. Es sei $\mathfrak{k}$ ein beliebiger Körper, $\mathfrak{N}$ ein über $\mathfrak{k}$ endlicher oder abzählbarer[16]) Abelscher Normalkörper. Ist von zwei beliebigen Zwischenkörpern $\mathfrak{L}$ und $\mathfrak{M}$ zwischen $\mathfrak{k}$ und $\mathfrak{N}$ stets der eine im andern enthalten, so soll $\mathfrak{N}$ über $\mathfrak{k}$ *zyklisch* heißen. Lassen sich die über $\mathfrak{k}$ zyklischen Körper $\mathfrak{Z}_1, \mathfrak{Z}_2, \ldots$ so bestimmen, daß $\mathfrak{N}$ der Vereinigungskörper aller $\mathfrak{Z}_i$ wird, und daß gleichzeitig $\mathfrak{Z}_i$ für jedes i mit dem Vereinigungskörper $\mathfrak{M}_i$ aller $\mathfrak{Z}_k (k \neq i)$ gerade den Durchschnitt $\mathfrak{k}$ besitzt, so sagen wir, es sei $\mathfrak{N}$ über $\mathfrak{k}$ *zyklisch direkt zerlegbar*. Dann gilt der (wohlbekannte) Satz:

Die Galoissche Gruppe Γ von $\mathfrak{N}$ über $\mathfrak{k}$ ist ein separable abgeschlossene Gruppe. $\mathfrak{N}$ ist dann und nur dann über $\mathfrak{k}$ zyklisch bzw. zyklisch direkt zerlegbar, wenn Γ zyklisch bzw. zyklisch direkt zerlegbar ist.

[15a]) *Zusatz bei der Korrektur:* Inzwischen habe ich eine Gruppe der genannten Art gefunden. Die im folgenden Satz erwähnte „gefühlsmäßig bezweifelte" Möglichkeit ist also tatsächlich ausgeschlossen.

[16]) Es soll also $\mathfrak{N}$ aus $\mathfrak{k}$ durch Adjunktion von endlich oder abzählbar unendlich vielen Elementen hervorgehen. Der Fall der endlich vielen Elemente entspricht natürlich den — nach Anm. [5]) auch zu den separablen gehörigen — endlichen Abelschen Gruppen.

Außerdem überzeugt man sich leicht, daß eine Galoissche Gruppe Γ niemals Elemente unendlicher Höhe enthält. Aus den oben besprochenen allgemeinen Theoremen ergibt sich daher sofort durch Spezialisierung:

Ist E *die zur Galoisschen Gruppe* Γ *von* $\mathfrak{R}$ *über* $\mathfrak{k}$ *gehörige Knotengruppe, so ist* $\mathfrak{R}$ *über* $\mathfrak{k}$ *dann und nur dann zyklisch direkt zerlegbar, wenn* Γ/E *unverknotet ist.*

Mit diesem Satze ist natürlich noch nicht gezeigt, daß $\mathfrak{R}$ nicht immer über $\mathfrak{k}$ zyklisch direkt zerlegbar zu sein braucht; aber diese Lücke kann leicht durch Konstruktion eines geeigneten Beispiels ausgefüllt werden. Es sei $\mathfrak{k}$ ein beliebiger Körper, der die sämtlichen p^k-ten Einheitswurzeln $e_k = e^{\frac{2\pi i}{p^k}}$ $(k = 1, 2, \ldots)$ enthält; $u, v_1, v_2, v_3, \ldots$ seien abzählbar viele Unbestimmte, $\mathfrak{k}$ bedeute den Körper $\mathfrak{k}_0(u, v_1, v_2, \ldots)$, unter t_k $(k = 1, 2, \ldots)$ möge eine Nullstelle des über $\mathfrak{k}$ irreduziblen Polynoms $x^{p^{k+1}} - u \cdot v_k^p$ verstanden werden. Setzen wir dann $\mathfrak{R} = \mathfrak{k}(t_1, t_2, \ldots)$, so erweist sich die Gruppe Γ von $\mathfrak{R}$ über $\mathfrak{k}$ als isomorph zu der in Anm. [14]) konstruierten Gruppe A. [17])

Es ist also $\mathfrak{R}$ *trotz seines äußerst einfachen Baues über* $\mathfrak{k}$ *nicht zyklisch direkt zerlegbar*, — ein auf den ersten Blick ziemlich überraschendes Ergebnis, das den Schluß unserer Betrachtungen bilden soll.

---

[17]) Es sei $v = u^{\frac{1}{p}}$, $\mathfrak{L} = \mathfrak{k}(v)$, und es bedeute α_l diejenige Selbstabbildung von $\mathfrak{R}$ über $\mathfrak{L}$, die durch die Zuordnungen $v \to v$, $t_k \to t_k$ $(k \neq l)$, $t_l \to e_l \cdot t_l$ definiert wird; $\mathsf{Z}_l = (\alpha_l)$ sei die zyklische Untergruppe der Ordnung p^l von Γ mit dem erzeugenden Element α_l. Dann besitzt die (natürlich additiv geschriebene) Galoissche Gruppe Δ von $\mathfrak{R}$ über $\mathfrak{L}$ die direkte Summenzerlegung $\Delta = \mathsf{Z}_1 + \mathsf{Z}_2 + \cdots$, es entspricht Δ also genau der Gruppe A_1 des Beispiels von Anm. [14]). — Es sei ferner ξ die durch die Zuordnungen $v \to e_1 \cdot v$, $t_k \to e_{k+1} \cdot t_k$ $(k = 1, 2, \ldots)$ definierte Selbstabbildung von $\mathfrak{R}$ über $\mathfrak{k}$. Dann wird einerseits offenbar $\Gamma = \Delta(\xi)$, und man hat andrerseits

$$p \cdot \xi = \alpha_1 + \alpha_2 + \alpha_3 + \cdots,$$

weil die p-malige Ausführung der Selbstabbildung ξ zu den Zuordnungen $v \to v$, $t_k \to e_k \cdot t_k$ $(k = 1, 2, \ldots)$ führt.

Eingegangen 4. Januar 1940.

Zusatz bei der Korrektur. Die in der Galoisschen Theorie allein auftretenden separablen Gruppen ohne Elemente unendlicher Höhe können topologisch gekennzeichnet werden als die einzigen *kompakten* separablen Gruppen. Darüber hinaus läßt sich zeigen, daß die Klasse der kompakten separablen Gruppen im Sinne unserer Note identisch ist mit der Klasse der kompakten nulldimensionalen Gruppen (mit zweitem Abzählbarkeitsaxiom) im Sinne von Pontrjeagin [6]). — Bei dem in [15]) erwähnten Gegenbeispiel gegen die Pietrkowskischen Sätze handelt es sich genau um dieselbe Gruppe wie in [14]); doch sind die Überlegungen, die im Text zur Aufstellung dieser Gruppe führten, von den Überlegungen Pontrjeagins völlig verschieden. Nach Pontrjeagin sind bekanntlich die nulldimensionalen kompakten Gruppen (mit zweitem Abzählbarkeitsaxiom) dual zu den abzählbaren gewöhnlichen Abelschen Gruppen ohne Elemente unendlicher Ordnung. Verknüpft man das Pontrjeaginsche Dualitätsprinzip mit den andersartigen Ansätzen unserer Note, so kommt man zu bemerkenswerten neuen Ergebnissen, auf die ich in einer späteren Veröffentlichung genauer eingehen werde. — Bei den von Elementen unendlicher Höhe nicht freien separablen Gruppen dürften sich keine näheren Beziehungen zu den Untersuchungen Pontrjeagins und seiner Nachfolger ergeben. Denn die nichtkompakten separablen Gruppen sind i. a. weder lokal kompakt noch bikompakt noch lokal bikompakt.

Darstellungstheorie der endlichen Gruppen.

Von *Wilhelm Specht* in Breslau.

Die Grundaufgabe der Darstellungstheorie ist die Bestimmung aller zu einer vorgegebenen abstrakten endlichen Gruppe $\mathfrak{G}$ homomorphen Gruppen von Matrizen eines beliebigen Grades, deren Elemente aus dem minimalen algebraisch-abgeschlossenen Körper über einem beliebigen Primkörper stammen. Jedem Element A aus $\mathfrak{G}$ wird daher durch eine Darstellung eine Matrix $D(A)$ zugeordnet mit der Maßgabe, daß für jedes Paar A, B aus $\mathfrak{G}$

$$D(AB) = D(A)D(B)$$

gelten soll. Man kann sich sogleich auf den Fall beschränken, daß dem Einheitselement 1 der Gruppe die Einheitsmatrix $D(1) = E$ zugeordnet ist, so daß alle Matrizen $D(A)$ der Darstellung regulär sind.

Zwei Darstellungen $D_1(A)$, $D_2(A)$ einer Gruppe $\mathfrak{G}$ heißen *ähnlich*, wenn mit einer konstanten regulären Matrix P die Gleichung

$$P^{-1}D_1(A)\,P = D_2(A)$$

für alle A aus $\mathfrak{G}$ besteht; einander nicht ähnliche Darstellungen wollen wir auch als *wesentlich verschieden* bezeichnen.

Eine Darstellung $D(A)$ der Gruppe $\mathfrak{G}$ heißt *reduzibel*, wenn eine zu $D(A)$ ähnliche Darstellung von der Gestalt

$$P^{-1}D(A)P = \begin{pmatrix} D_1(A) & 0 \\ D_{21}(A) & D_2(A) \end{pmatrix}$$

vorhanden ist; hierin bilden die Teilmatrizen $D_1(A)$ und $D_2(A)$ wieder Darstellungen der Gruppe $\mathfrak{G}$. Im gegenteiligen Falle ist $D(A)$ *irreduzibel*. Weiter heißt die Darstellung $D(A)$ *zerfällbar*, wenn eine zu ihr ähnliche Darstellung der Gestalt

$$P^{-1}D(A)P = \begin{pmatrix} D_1(A) & 0 \\ 0 & D_2(A) \end{pmatrix}$$

vorhanden ist, *unzerfällbar*, wenn dies nicht zutrifft. Durch das erste Verfahren wird eine Darstellung in ihre irreduziblen Bestandteile zerlegt, die abgesehen von der Reihenfolge und Ähnlichkeitstransformationen eindeutig bestimmt sind; ebenso wird durch das zweite Verfahren die Darstellung in ihre unzerfällbaren Bestandteile zerlegt, die gleichfalls abgesehen von der Reihenfolge und Ähnlichkeitstransformationen eindeutig bestimmt sind. Stimmen bei einer Darstellung die unzerfällbaren mit den irreduziblen Bestandteilen überein, so heißt sie *vollreduzibel*. Sind die Darstellungen einer Gruppe $\mathfrak{G}$ sämtlich vollreduzibel, so läßt sich demgemäß die Aufgabe der Darstellungstheorie auf die Bestimmung aller irreduziblen Darstellungen zurückführen, während man andernfalls auf die Bestimmung der unzerfällbaren Darstellungen eingehen muß, eine Aufgabe, die wesentlich größere Schwierigkeiten mit sich bringt.

Die Darstellungstheorie der endlichen Gruppen im Körper Ω_0 der komplexen Zahlen hat als erster G. Frobenius entwickelt und in ihren Hauptzügen vollständig durchgeführt. Die Grundergebnisse lassen sich in der folgenden Gestalt zusammenfassen:

(1) Jede Darstellung einer endlichen Gruppe $\mathfrak{G}$ in Ω_0 ist vollreduzibel.

(2) Die Anzahl der wesentlich verschiedenen irreduziblen Darstellungen in Ω_0 ist gleich der Anzahl k der Klassen ähnlicher Elemente in $\mathfrak{G}$.

(3) Die reguläre Darstellung enthält jede irreduzible Darstellung genau so oft, wie ihr Grad angibt. Dabei versteht man unter der regulären Darstellung die Darstellung

$$R(A) = (\delta_{PAQ^{-1}})$$

vom Grade g der Gruppe $\mathfrak{G}$, worin

$$\delta_A = 0 \quad \text{für} \quad A \neq 1; \quad \delta_1 = 1$$

zu setzen ist und P, Q unabhängig voneinander die Elemente von $\mathfrak{G}$ in der gleichen beliebig festgesetzten Reihenfolge durchlaufen.

Versteht man ferner unter dem *Charakter* $\chi(A)$ der Darstellung $D(A)$ die Menge der Werte

$$\chi(A) = Spur\ D(A),$$

so gilt:

(4) Darstellungen gleichen Charakters sind ähnlich.

(5) Die Charaktere

$$\chi_1(A),\ \chi_2(A), \ldots,\ \chi_k(A)$$

der wesentlich verschiedenen irreduziblen Darstellungen genügen den Relationen

$$\frac{1}{g}\sum_R \chi_\varkappa(R)\,\chi_\lambda(R^{-1}) = \begin{Bmatrix} 0 & (\varkappa \neq \lambda) \\ 1 & (\varkappa = \lambda) \end{Bmatrix} \quad (\varkappa, \lambda = 1, 2, \ldots, k),$$

worin R alle Elemente von $\mathfrak{G}$ durchläuft.

Die Begründung dieser Ergebnisse stützt sich hauptsächlich auf den *Verkettungssatz* von I. Schur, nach dem zwischen zwei irreduziblen Darstellungen $D_1(A)$, $D_2(A)$ von $\mathfrak{G}$ eine Verkettung

$$PD_1(A) = D_2(A)P$$

mit einer von der Nullmatrix verschiedenen konstanten Matrix P für alle Elemente A aus $\mathfrak{G}$ nur für ähnliche Darstellungen bestehen kann, auf den *Satz von Frobenius-Schur*, der aussagt, daß eine lineare Beziehung

$$a_1\,\chi_1(A) + a_2\,\chi_2(A) + \cdots + a_k\,\chi_k(A) = 0$$

für die Charaktere der irreduziblen Darstellungen nur bei

$$a_1 = a_2 = \cdots = a_k = 0$$

gilt, und auf den *Satz von Maschke*, der die volle Reduzibilität jeder endlichen Matrixgruppe feststellt.

Die Darstellungstheorie einer endlichen Gruppe $\mathfrak{G}$ läßt sich mit genau den gleichen Ergebnissen in dem minimalen algebraisch-abgeschlossenen Körper Ω_p über dem Primkörper P_p der Primzahlcharakteristik p in dem Falle vollständig durchführen, daß die Primzahl p in der Ordnung g der Gruppe $\mathfrak{G}$ nicht aufgeht. Vollständig andere Verhältnisse trifft man indes in dem noch verbleibenden Falle an, daß p in g aufgeht; diese Änderung der Ergebnisse hat ihren Grund vor allem in der Tatsache, daß hier der Satz von Maschke nicht mehr allgemein gültig ist, so daß die vollständige Durchführung der Theorie die Bestimmung aller unzerfällbaren Darstellungen erfordert. Der Verkettungssatz und der Satz von Frobenius-Schur stehen dagegen auch in diesem Falle in vollem Umfange zur Verfügung.

Die ersten und bisher einzigen allgemeinen und ausführlicheren Untersuchungen dieses schwierigsten Sonderfalles der Darstellungstheorie endlicher Gruppen in einem algebraisch-abgeschlossenen Körper Ω_p, deren Charakteristik p in der Gruppenordnung aufgeht, verdankt man R. Brauer und C. Nesbitt. Der Bericht über ihre Ergebnisse soll den Inhalt meines Vortrages bilden.

Sind

$$D_1(A),\ D_2(A),\ \ldots,\ D_s(A)$$

wesentlich verschiedene irreduzible Darstellungen einer Gruppe $\mathfrak{G}$ im Körper Ω_p mit den Charakteren

$$\chi_1(A),\ \chi_2(A),\ \ldots,\ \chi_s(A),$$

so kann auf Grund des Satzes von Frobenius-Schur eine lineare Beziehung[1])

$$a_1\,\chi_1(A) + a_2\,\chi_2(A) + \cdots + a_s\,\chi_s(A) \equiv 0$$

nur für

$$a_1 \equiv a_2 \equiv \cdots \equiv a_s \equiv 0$$

bestehen. Zwei irreduzible Darstellungen sind daher dann und nur dann ähnlich, wenn ihre Charaktere übereinstimmen. Ferner folgt hieraus leicht das folgende *Lemma*, auf das sich die weiterhin geschilderten Ergebnisse hauptsächlich stützen:

Haben in zwei Darstellungen $D_1(A)$ und $D_2(A)$ einer Gruppe $\mathfrak{G}$ die beiden Matrizen $D_1(A)$, $D_2(A)$ für jedes A aus $\mathfrak{G}$ die gleichen charakteristischen Wurzeln, so besitzen die beiden Darstellungen die gleichen irreduziblen Bestandteile.

Da diese Aussage für irreduzible Darstellungen unmittelbar klar ist, kann der Beweis induktiv geführt werden. Sicherlich ist

$$Spur\ D_1(A) \equiv Spur\ D_2(A).$$

Ist daher

$$Spur\ D_1(A) \equiv \sum_\lambda a_\lambda\,\chi_\lambda(A), \qquad Spur\ D_2(A) \equiv \sum_\lambda b_\lambda\,\chi_\lambda(A)$$

mit den Charakteren $\chi_\lambda(A)$ der in beiden Darstellungen vorkommenden irreduziblen Darstellungen, so ist $a_\lambda \equiv b_\lambda$. Beschränkt man sich auf vollreduzible Darstellungen, was hier ohne weiteres erlaubt ist, da nur eine Aussage über die irreduziblen Bestandteile der beiden Darstellungen gemacht wird, so läßt sich die Beweisführung sehr leicht auf den Fall zurückführen, daß

$$a_\lambda = 0;\quad b_\lambda \equiv 0 \quad \text{oder} \quad a_\lambda \equiv 0;\quad b_\lambda = 0$$

ist. Durch Übergang zu Darstellungen mit den Charakteren

$$\sum_\lambda \frac{a_\lambda}{p}\,\chi_\lambda(A),\quad \sum_\lambda \frac{b_\lambda}{p}\,\chi_\lambda(A)$$

ergibt sich dann sofort der Beweis.

Darstellungen einer vorgegebenen Gruppe $\mathfrak{G}$ im Körper Ω_p lassen sich sehr leicht aus Darstellungen in Ω_0 auf dem folgenden Wege gewinnen: Es sei $D(A)$ eine in einem endlichen algebraischen Zahlkörper K rationale Darstellung der Gruppe $\mathfrak{G}$, von der ohne weiteres (nach etwaiger Erweiterung des Körpers K) angenommen werden kann, daß die Matrizen $D(A)$ aus lauter ganzalgebraischen Zahlen bestehen. Ist dann $\mathfrak{p}$ ein Primideal in K, für das

$$p \equiv 0\ (\mathfrak{p})$$

[1]) Ich gebrauche als Gleichheitszeichen: $=$ in Ω_0, $\equiv$ in Ω_p.

ist, so bilden die Restklassen mod $\mathfrak{p}$ einen endlichen Körper der Charakteristik p. Durch Übergang zu den Restklassen erhalten wir demnach aus $D(A)$ eine Darstellung $\tilde{D}(A)$ in einem Körper der Charakteristik p:

$$D(A) \underset{\mathfrak{p}}{\rightarrow} \tilde{D}(A).$$

Die Darstellung $\tilde{D}(A)$ hängt in ihrer Gestalt wesentlich von der Wahl des Primideals $\mathfrak{p}$ ab. Sind $\mathfrak{p}, \mathfrak{p}_1$ zwei Primideale in K, die p enthalten, und ist

$$D(A) \underset{\mathfrak{p}}{\rightarrow} \tilde{D}(A), \qquad D(A) \underset{\mathfrak{p}_1}{\rightarrow} \tilde{D}_1(A),$$

so brauchen $\tilde{D}(A)$ und $\tilde{D}_1(A)$ einander nicht ähnlich zu sein; wohl aber gibt es stets eine zu $D(A)$ ähnliche Darstellung $D^*(A) = P^{-1}D(A)P$ derart, daß

$$D^*(A) \underset{\mathfrak{p}_1}{\rightarrow} \tilde{D}^*(A)$$

mit einer zu $\tilde{D}(A)$ ähnlichen Darstellung $\tilde{D}^*(A)$ gilt.

Sind $D(A)$ und $D_1(A)$ zwei in Ω_0 ähnliche Darstellungen von $\mathfrak{G}$, die in K bzw. K_1 rational sind, ferner

$$D(A) \underset{\mathfrak{p}}{\rightarrow} \tilde{D}(A) \text{ in } \mathsf{K}$$
$$D_1(A) \underset{\mathfrak{p}_1}{\rightarrow} \tilde{D}_1(A) \text{ in } \mathsf{K}_1,$$

so sind die beiden Darstellungen $\tilde{D}(A)$ und $\tilde{D}_1(A)$ in Ω_p nicht notwendig ähnlich. Man kann aber, falls $\mathfrak{p}$ vorgegeben ist, stets in K_1 ein Primideal $\mathfrak{p}_1$ so angeben, daß $\tilde{D}_1(A)$ die gleichen irreduziblen Bestandteile wie $\tilde{D}(A)$ besitzt. Man hat dazu nur einen gemeinsamen Erweiterungskörper K^* von K und K_1 zu wählen, der die charakteristischen Wurzeln aller Matrizen $D(A)$ und $D_1(A)$ enthält; ist dann $\mathfrak{p}^*$ ein Primteiler von $\mathfrak{p}$ in K^*, so bestimme man $\mathfrak{p}_1$ so, daß

$$\mathfrak{p}^* \equiv 0 \ (\mathfrak{p}_1).$$

Nun sei

$$D_1(A), D_2(A), \ldots, D_k(A)$$

ein Satz wesentlich verschiedener irreduzibler Darstellungen der Gruppe $\mathfrak{G}$ in Ω_0 von den Graden

$$d_1, d_2, \ldots, d_k;$$

wir können annehmen, daß diese Darstellungen sämtlich in dem endlichen algebraischen Körper K rational sind und ihre Matrizen aus ganzen algebraischen Zahlen dieses Körpers bestehen. Ist dann $\mathfrak{p}$ ein (fest gewählter) Primteiler von p in K, so sei

$$D_\varkappa(A) \underset{\mathfrak{p}}{\rightarrow} \tilde{D}_\varkappa(A).$$

Ferner sei

$$F_1(A), \ F_2(A), \ldots, F_l(A)$$

ein Satz wesentlich verschiedener irreduzibler Darstellungen von $\mathfrak{G}$ in Ω_p von den Graden

$$f_1, f_2, \ldots, f_l.$$

Es gelten dann mit gewissen nichtnegativen ganzen Zahlen die Zerlegungsgleichungen[2])

$$\tilde{D}(A) \doteq \sum_\lambda d_{\varkappa\lambda} F_\lambda(A).$$

Die *Zerlegungszahlen* $d_{\varkappa\lambda}$ fassen wir zu einer Matrix

$$D = (d_{\varkappa\lambda})$$

von k Zeilen und l Spalten zusammen.

---

[2]) Die Gleichung $D(A) \doteq \sum_\lambda a_\lambda F_\lambda(A)$ soll besagen, daß $D(A)$ den irreduziblen Bestandteil $F_\lambda(A)$ genau a_λ-fach enthält.

Die reguläre Darstellung $R(A)$ der Gruppe $\mathfrak{G}$ kann sogleich als Darstellung $\tilde{R}(A)$ im Primkörper P_p aufgefaßt werden. Aus der Zerfällung von $R(A)$ und $\tilde{R}(A)$ in ihre irreduziblen Bestandteile

$$R(A) \doteq \sum_{\varkappa} d_\varkappa D_\varkappa(A), \qquad \tilde{R}(A) \doteq \sum_{\lambda} u_\lambda F_\lambda(A)$$

erhalten wir dann

$$u_\lambda = \sum_{\varkappa} d_\varkappa d_{\varkappa\lambda}.$$

Wie man leicht zeigen kann, sind in $\tilde{R}(A)$ alle irreduziblen Darstellungen $F_\lambda(A)$ enthalten, also alle u_λ von Null verschieden. Daher ist auch für jedes λ wenigstens ein $d_{\varkappa\lambda}$ von Null verschieden. Man erhält daher alle in Ω_p irreduziblen Darstellungen schon dadurch, daß man die in Ω_0 irreduziblen Darstellungen nach dem oben beschriebenen Verfahren in Darstellungen in Ω_p verwandelt und diese ausreduziert. Eine volle Zerfällung der regulären Darstellung $\tilde{R}(A)$ in Ω_p läßt sich nicht erreichen, da der Satz von Maschke nicht zur Verfügung steht. Zerlegt man $\tilde{R}(A)$ in seine unzerfällbaren Bestandteile, so kommen in dieser Darstellung genau l wesentlich verschiedene unzerfällbare Bestandteile

$$U_1(A), U_2(A), \ldots, U_l(A)$$

vor; bei passender Reihenfolge besitzt für $\lambda = 1, 2, \ldots, l$ jedes $U_\lambda(A)$ den Grad u_λ und tritt in $\tilde{R}(A)$ genau f_λ-fach auf. Zum Beweise dieses Zerlegungssatzes werden die beiden regulären Darstellungen

$$\tilde{R}(A) = (\delta_{PAQ-1}), \quad \tilde{S}(A) = (\delta_{Q-1AP}),$$

die bekanntlich die Vertauschungsbeziehung

$$\tilde{R}(A)\tilde{S}(B) = \tilde{S}(B)\tilde{R}(A)$$

erfüllen, gegenseitig zerlegt.

Jede der Darstellungen $U_\lambda(A)$ kann (bei geeigneter Reihenfolge) nach ihren irreduziblen Bestandteilen derart zerlegt werden, daß die irreduzible Darstellung $F_\lambda(A)$ jeweils in $U_\lambda(A)$ als erster und letzter Bestandteil auftritt. Setzen wir nach dieser Festsetzung der Numerierung

$$U_\lambda(A) \doteq \sum_{\mu=1}^{l} c_{\lambda\mu} F_\mu(A),$$

so erfüllen die *Cartan-Invarianten* $c_{\lambda\mu}$ der Gruppe $\mathfrak{G}$ die Beziehung

$$c_{\lambda\mu} = \sum_{\varkappa} d_{\varkappa\lambda} d_{\varkappa\mu};$$

in Matrixform kann dies auch in der Gestalt

$$C = D'\,D$$

geschrieben werden, wenn $C = (c_{\lambda\mu})$ gesetzt wird. Insbesondere erkennt man hieraus die Symmetrie der Matrix C. Der Beweis dieser Gleichung geht aus Frobeniusschen Zerlegungssätzen über die Determinante

$$\det\left(\tilde{R}'(y) + \tilde{S}(x)\right)$$

der Gruppenmatrizen

$$R(x) = \sum_{A} x_A R(A), \quad S(x) = \sum_{A} x_A S(A)$$

durch einfache Abzählung hervor.

Es bleibt noch als eine wesentliche Aufgabe die Bestimmung der Anzahl l der irreduziblen Darstellungen der Gruppe $\mathfrak{G}$ im Körper Ω_p. Zu diesem Zwecke bezeichnen wir die Ähnlichkeitsklassen von $\mathfrak{G}$ mit

$$(1), (2), \ldots, (k),$$

wobei wir ihre Zählung derart einrichten, daß die ersten h Klassen genau die Elemente von $\mathfrak{G}$ enthalten, die eine zu p teilerfremde Ordnung besitzen. Dann kann das Lemma auch in der folgenden Gestalt ausgesprochen werden:

Haben in zwei Darstellungen $D_1(A)$ und $D_2(A)$ einer Gruppe $\mathfrak{G}$ die beiden Matrizen $D_1(M)$, $D_2(M)$ für alle Elemente M der ersten h Klassen von $\mathfrak{G}$ die gleichen charakteristischen Wurzeln, so besitzen die beiden Darstellungen die gleichen irreduziblen Bestandteile.

Denn jedes Element A der Gruppe $\mathfrak{G}$ kann als Produkt

$$A = PM = MP$$

dargestellt werden, worin P ein Element von Primzahlpotenzordnung p^α ist und M aus den ersten h Klassen stammt. Dann besitzen $D_1(A)$ und $D_2(A)$ die gleichen charakteristischen Wurzeln wie $D_1(M)$ bzw. $D_2(M)$.

Diese Tatsache läßt eine neue Erklärung des Charakters einer Darstellung $D(A)$ vom Grade n in Ω_p zu. Ist M ein Element der ersten h Klassen von der Ordnung g', ist also $(g', p) = 1$, so sind die Wurzeln von $D(M)$ Einheitswurzeln der Ordnung g'. Wir ersetzen sie durch die ihnen entsprechenden komplexen Einheitswurzeln ε_ν gleichen Grades und erklären als Charakterwert $\chi(M)$ die Zahl

$$\chi(M) = \sum_\nu \varepsilon_\nu \qquad (\nu = 1, 2, \ldots, n).$$

Durch die Zahlen

$$\chi(M),\ \chi(M^2), \ldots,\ \chi(M^n)$$

sind dann die Wurzeln ε_ν, also auch die Wurzeln der Matrix $D(M)$ eindeutig bestimmt. Nennen wir daher die Menge aller Werte $\chi(M)$ den Charakter der Darstellung $D(A)$ von $\mathfrak{G}$, so folgt aus dem Lemma unmittelbar:

Zwei Darstellungen haben dann und nur dann die gleichen irreduziblen Bestandteile, wenn sie den gleichen Charakter besitzen.

Haben nun die Darstellungen $\tilde{D}_\varkappa(A)$ die Charaktere $\varphi_\varkappa(A)$, die Darstellungen $F_\lambda(A)$ die Charaktere $\chi_\lambda(A)$, so ist

$$\varphi_\varkappa(A) = \sum_\lambda d_{\varkappa\lambda}\, \chi_\lambda(A)$$

und weiter, wenn $\Phi_\lambda(A)$ den Charakter von $U_\lambda(A)$ bezeichnet:

$$\Phi_\lambda(A) = \sum_\mu c_{\lambda\mu}\, \chi_\mu(A), \qquad \Phi_\lambda(A) = \sum_\varkappa d_{\varkappa\lambda}\, \varphi_\varkappa(A).$$

Aus den Beziehungen für $\varphi_\varkappa(A)$ erhält man nun leicht:

$$\sum_\lambda \Phi_\lambda(M)\, \chi_\lambda(N^{-1}) = \delta_{MN^{-1}}\, \frac{g}{g_M},$$

wenn M, N den ersten h Klassen entstammen und g_M die Anzahl der Elemente der Klasse bezeichnet, der M angehört. Hieraus folgt sogleich, daß $l \geqq h$ sein muß. Andererseits kann h nicht kleiner als l sein, da sonst das Gleichungssystem

$$\sum_\lambda \chi_\lambda(M_\varrho) z_\lambda = 0 \qquad (\varrho = 1, 2, \ldots, h)$$

für Vertreter M_ϱ der ersten h Klassen eine nichttriviale Lösung besäße. Dann wäre aber auch für alle Elemente A aus $\mathfrak{G}$

$$\sum_\lambda \bar{z}_\lambda\, \chi_\lambda(A) \equiv 0,$$

im Widerspruch zum Satze von Frobenius-Schur. Es gilt demnach der Satz:

Die Anzahl der wesentlich verschiedenen irreduziblen Darstellungen einer Gruppe $\mathfrak{G}$ in Ω_p ist gleich der Anzahl l der Ähnlichkeitsklassen von $\mathfrak{G}$, die Elemente einer zu p teilerfremden Ordnung enthalten.

Durch einfache Rechnung lassen sich noch die folgenden Beziehungen nachweisen:

$$\sum_{\varrho,\sigma} \chi_\varrho(\varkappa)\chi_\sigma(\lambda')c_{\varrho\sigma} = \frac{g}{g_\varkappa}\delta_{\varkappa\lambda},$$

worin (λ') die zu (λ) reziproke Klasse, $(\varkappa)$, (λ) zwei der ersten h Klassen bezeichnen, $g_\varkappa$ die Anzahl der Elemente von $(\varkappa)$ bedeutet und

$$\delta_{\varkappa\lambda} = 0 \quad \text{für} \quad \varkappa \neq \lambda; \qquad \delta_{\varkappa\varkappa} = 1$$

zu setzen ist, sowie

$$\sum_{\varrho} g_\varrho \chi_\varkappa(\varrho)\chi_\lambda(\varrho') = g\gamma_{\varkappa\lambda},$$

wobei $C^{-1} = (\gamma_{\varkappa\lambda})$ die Inverse zu C bedeutet.

Schrifttum.

R. Brauer, Über die Darstellung von Gruppen in Galoisschen Feldern, Actualités scient. **195** (1935).

R. Brauer and C. Nesbitt, On the regular representations of algebras, Proceedings Nat. Acad. USA **23** (1937), 236—240.

R. Brauer and C. Nesbitt, On the modular representations of groups of finite order I., Univ. of Toronto studies, Math. ser. Nr. 4 (1937).

L. E. Dickson, On the group defined for any given field by the multiplication table of any given finite group, Transactions Amer. Math. Soc. **3** (1902), 285—301.

L. E. Dickson, Modular theory of group-characters, Bulletin Amer. Math. Soc. (2) **13** (1907), 477—488.

L. E. Dickson, Modular theory of group-matrices, Transactions Amer. Math. Soc. **8** (1907), 389—398.

G. Frobenius, Über Gruppencharaktere, Sitzungsber. Akad. Berlin 1896, 985—1021.

G. Frobenius, Über die Darstellung der endlichen Gruppen durch lineare Substitutionen I., Sitzungsber. Akad. Berlin 1897, 994—1015; II., Sitzungsber. Akad. Berlin 1899, 482—500.

G. Frobenius und I. Schur, Über die Äquivalenz der Gruppen linearer Substitutionen, Sitzungsber. Akad. Berlin 1906, 209—217.

H. Maschke, Beweis des Satzes, daß diejenigen endlichen linearen Substitutionsgruppen, in welchen einige durchgehends verschwindende Coefficienten auftreten, intransitiv sind, Math. Ann. **52** (1899), 363—368.

I. Schur, Neue Begründung der Theorie der Gruppencharaktere, Sitzungsber. Akad. Berlin 1905, 406—432.

Eingegangen 30. August 1939.

Soeben erschien:

Lehrbuch der Mathematik

zum Selbstunterricht und für Studierende der Naturwissenschaften und der Technik

Eine Einführung

in die Differential- und Integralrechnung und in die analytische Geometrie

Von

Professor Dr. Dr.-Ing. Georg Scheffers

8. Auflage. Mit 438 Figuren. Lexikon-Oktav. VIII, 743 Seiten. Geb. RM 15.—

Dieses Lehrbuch ist für alle diejenigen geschrieben, denen die Mathematik eine Hilfswissenschaft ist, namentlich für Studierende der Naturwissenschaften und der Technik. Da es in erster Linie für das Selbststudium bestimmt ist, geht es von dem geringsten Maß von Vorkenntnissen aus: der Leser braucht nur im Buchstabenrechnen, in der Auflösung von Gleichungen ersten Grades mit einer Unbekannten und in der niederen Geometrie bewandert zu sein. Das Ziel des Buches ist, den Anfänger von dem niedrigsten Stand an Vorkenntnissen zu einer solchen Höhe zu bringen, daß er nach dem Studium dieses Buches fähig ist, die in seinem besonderen Forschungsgebiet auftretenden Anwendungen der Mathematik zu verstehen und, wenn er es brauchen sollte, schwierigere mathematische Literatur mit Verständnis zu lesen

---

Verlag Walter de Gruyter & Co., Berlin W 35

Geschichte der Elementar-Mathematik

in systematischer Darstellung mit besonderer Berücksichtigung der Fachwörter

Von

Dr. Johannes Tropfke†

Soeben erschien:

Band 4: Ebene Geometrie. Dritte, verbesserte und vermehrte Auflage, besorgt von Dr. Kurt Vogel. IV, 316 Seiten. RM 12.—, geb. RM 13.—

Früher sind erschienen:

Band 1: Rechnen. VII, 222 Seiten. 3. Auflage. 1930. RM 12.—, geb. RM 13.20

Band 2: Allgemeine Arithmetik. IV, 266 Seiten. 3. Auflage. 1933. RM 12.—, geb. 13.20

Band 3: Proportionen, Gleichungen. IV, 239 Seiten. 3., verbesserte und vermehrte Auflage. 1937. RM 10.—, geb. RM. 11.—

Band 5: I. Ebene Trigonometrie. II. Sphärik und sphärische Trigonometrie. IV, 185 Seiten. 2. Auflage. 1923. RM 7.50, geb. RM 8.50

Band 6: Analysis, Analytische Geometrie. IV, 169 Seiten. 2. Auflage. 1924. RM. 7.—, geb. RM 8.—

Band 7: Stereometrie. Verzeichnisse. V, 128 Seiten. 2. Auflage. 1924. RM 6.50, geb. RM 7.50

Soeben erschien:

Mathematische Mußestunden

Von

Prof. Dr. Hermann Schubert

Eine Sammlung von Geduldspielen, Kunststücken und Unterhaltungsaufgaben mathematischer Natur. Neubearbeitet von Professor Dr. F. Fitting. 6. Auflage. 260 Seiten Geb. RM 4.80

Dieses bekannte, jetzt in der sechsten Auflage erscheinende Buch, wendet sich in erster Linie an den mathematischen Laien, den es in leichtfaßlicher und spannender Form in das Wesen der verbreiteten mathematischen Spiele einführen will. Doch sind auch einzelne Abschnitte aufgenommen, welche sich, oft durch kleineren Druck gekennzeichnet, hauptsächlich an den mathematisch interessierten Leser wenden und diesem Anregungen zu eigenen Untersuchungen auf dem Gebiet der Unterhaltungsmathematik geben wollen

---

Verlag Walter de Gruyter & Co., Berlin W 35

Anzeigenpreise n. Tarif 3. — Verantwortl. f. d. Anzeigenteil: Kurt Dittrich, Berlin. I. v. W. g.